การเพิ่มความมั่นคงของชุดซอฟต์แวร์โทรศัพท์ผ่านอินเทอร์เน็ตและการปรับปรุงโพรโทคอลซิพเพื่อป้องกันการจู่โจมซิพฟลัดดิ้ง

ร้อยตำรวจโทประดิษฐ์ วงศ์สกุล

เสนอต่อมหาวิทยาลัยมหาสารคาม เพื่อเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์
กันยายน 2558

การเพิ่มความมั่นคงของชุดซอฟต์แวร์โทรศัพท์ผ่านอินเทอร์เน็ตและการปรับปรุงโพรโทคอลซิพเพื่อป้องกันการจู่โจมซิพฟลัดดิ้ง

ร้อยตำรวจโทประดิษฐ์ วงศ์สกุล

เสนอต่อมหาวิทยาลัยมหาสารคาม เพื่อเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์
กันยายน 2558

คณะกรรมการสอบวิทยานิพนธ์ ได้พิจารณาวิทยานิพนธ์ของร้อยตำรวจโทประดิษฐ์ วงศ์สกุล แล้วเห็นสมควรรับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ ของมหาวิทยาลัยมหาสารคาม

คณะกรรมการสอบวิทยานิพนธ์

.....	ประธานกรรมการ
(ผศ.ดร.ฉัตรเกล้า เจริญผล)	(กรรมการบัณฑิตศึกษาประจำคณะ)
.....	กรรมการ
(อาจารย์ ดร.สมนึก พ่วงพรพิทักษ์)	(อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก)
.....	กรรมการ
(ผศ.ดร.พนิดา ทรงรัมย์)	(อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม)
.....	กรรมการ
(อาจารย์ ดร.คำรณ สุนัติ)	(ผู้ทรงคุณวุฒิ)

มหาวิทยาลัยอนุมัติให้รับวิทยานิพนธ์ฉบับนี้ เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ ของมหาวิทยาลัยมหาสารคาม

.....
(ผศ.ดร.สุจิน บุตรดีสุวรรณ)
คณบดีคณะวิทยาการสารสนเทศ

.....
(ศ.ดร.ประดิษฐ์ เทอดทูล)
คณบดีบัณฑิตวิทยาลัย
วันที่ 30 เดือน ก.ย. พ.ศ. 2558

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้ ได้รับทุนจาก “โครงการพัฒนาศักยภาพทางการวิจัย” หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิทยาการคอมพิวเตอร์ ประจำปีการศึกษา 2555

วิทยานิพนธ์ฉบับนี้สำเร็จสมบูรณ์ได้ด้วยความกรุณาและความช่วยเหลืออย่างสูงยิ่งจาก อาจารย์ ดร.สมนึก พ่วงพรพิทักษ์ อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก ผู้ช่วยศาสตราจารย์ ดร.พนิดา ทรงรัมย์ อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม อาจารย์ ดร.ฉัตรเกล้า เจริญผล ประธานกรรมการสอบ และ อาจารย์ ดร.คำรณ สุนัติ กรรมการผู้ทรงคุณวุฒิ

ขอขอบพระคุณ อาจารย์ ดร.สมนึก พ่วงพรพิทักษ์ อาจารย์ที่ปรึกษาผู้เชี่ยวชาญ ผู้ให้การช่วยเหลือเครื่องมือและสนับสนุนการวิจัย

ขอขอบพระคุณ พ่อบัวโรย วงศ์สกุล แม่น่วม วงศ์สกุล และครอบครัว ซึ่งเปิดโอกาสให้ได้รับการศึกษาเล่าเรียน ตลอดจนคอยช่วยเหลือและให้กำลังใจผู้วิจัยเสมอมาจนสำเร็จการศึกษา

ร้อยตรวจโทประดิษฐ์ วงศ์สกุล

ชื่อเรื่อง การเพิ่มความมั่นคงของชุดซอฟต์แวร์โทรศัพท์ผ่านอินเทอร์เน็ตและการปรับปรุงโพรโทคอลซิพเพื่อป้องกันการจู่โจมซิพฟลัดดิ้ง
ผู้วิจัย ร้อยตำรวจโทประดิษฐ์ วงศ์สกุล
ปริญญา วิทยาศาสตรมหาบัณฑิต **สาขาวิชา** วิทยาการคอมพิวเตอร์
กรรมการควบคุม อาจารย์ ดร.สมนึก พ่วงพรพิทักษ์
ผู้ช่วยศาสตราจารย์ ดร.พนิดา ทรงรัมย์
มหาวิทยาลัย มหาวิทยาลัยมหาสารคาม **ปีที่พิมพ์** 2558

บทคัดย่อ

ซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายอินเทอร์เน็ต เช่น Asterisk, FreeSWITCH และ Kamailo เป็นที่นิยมนำมาประยุกต์ใช้งาน เพราะมีข้อดีเรื่องการลดต้นทุนขององค์กร ไม่มีค่าใช้จ่ายในการนำมาใช้งาน ซึ่งจากการศึกษางานวิจัยก่อนหน้าได้มีหลายกลุ่มวิจัยได้การพัฒนาชุดซอฟต์แวร์ VoIP ขึ้นมาโดยมีวัตถุประสงค์หลักในเรื่องความสะดวก ในการติดตั้ง ใช้งานง่าย แต่ก็ยังพบปัญหาในด้านความมั่นคง ดังนั้นวิทยานิพนธ์นี้จึงมีจุดประสงค์ข้อแรกคือการพัฒนาชุดซอฟต์แวร์ VoIP โดยใช้ซอฟต์แวร์ FreeSWITCH เป็นฐานในการพัฒนา มุ่งแก้ไขปัญหาด้านความมั่นคง และความสะดวกในการติดตั้งใช้งาน ได้ตั้งชื่อให้ต้นแบบชุดซอฟต์แวร์นี้ว่า “ISANBox.F” จากนั้นได้ทำการประเมินประสิทธิภาพของระบบ ISANBox.F ทั้งในด้านความมั่นคงและด้านคุณภาพการให้บริการ ผลการทดลองแสดงให้เห็นถึงประสิทธิภาพด้านความมั่นคงที่ดีขึ้นและมีคุณภาพของเสียงอยู่ในระดับที่ดี นอกจากนี้ยังมีจุดประสงค์ข้อที่สองคือการเพิ่มประสิทธิภาพด้านความมั่นคงในระดับโพรโทคอลสัญญาณของ VoIP (Session Initiation Protocol: SIP) เพื่อป้องกันการโจมตีด้วยเทคนิคซิพฟลัดดิ้ง โดยการออกแบบแนวคิดเพื่อปรับปรุงให้โพรโทคอล SIP มีความสามารถในการตรวจจับการโจมตีได้ด้วยตัวเอง และทำการทดสอบประสิทธิภาพของแนวคิดในเครือข่ายจำลอง (Test-beds) ซึ่งผลการทดสอบประสิทธิภาพเมื่อเปรียบเทียบกับวิธีการแก้ปัญหาก่อนหน้า แสดงให้เห็นว่าแนวคิดที่ได้เสนอในวิทยานิพนธ์สามารถแก้ไขปัญหาการโจมตี SIP Flooding ได้ดี และมีการตอบสนองต่อการโจมตีได้ดียิ่งขึ้น

คำสำคัญ: ชุดซอฟต์แวร์โทรศัพท์ผ่านอินเทอร์เน็ต; ความมั่นคงของระบบวีโอไอพี; โพรโทคอลสัญญาณสำหรับโทรศัพท์ผ่านอินเทอร์เน็ต; การจู่โจมซิพฟลัดดิ้ง

TITLE Security Enhancement of a VoIP Software Package and
SIP Improvement to Protect against SIP Flooding Attacks
AUTHOR Pol.Lt.Pradit Wongsakul
DEGREE Master of Science **MAJOR** Computer Science
ADVISORS Somnuk Puangpronpitag, Ph.D.
Panida Songram, Ph.D.
UNIVERSITY Mahasarakham University **YEAR** 2015

ABSTRACT

Voice over IP (VoIP) open-source software (such as Asterisk, FreeSWITCH, Kamailo) has been widely deployed due to its useful features and freeness of cost. Several previous studies have also tried to build software packages over the VoIP open-source software. Their main purpose is to ease the installation and user interface. However, several VoIP software packages have still suffered with the security issues. So, the first aim of this thesis is to enhance the security of VoIP software package, based on FreeSWITCH. The prototype has also been implemented and named “ISANBox.F”. Furthermore, the experiments have been done on a test-bed to evaluate ISANBox.F for both security and the quality of voice issues. The experimental results have demonstrated the enhanced security and a good quality of voice. Moreover, the second aim of this thesis is to enhance the security of VoIP signaling protocol (Session Initiation Protocol: SIP) to protect against SIP flooding attacks. Hence, SIP modification has been designed to detect and protect the SIP flooding attacks. The experiments on a test-bed have done to evaluate the proposed design. In comparison to the previous solutions of SIP flooding attacks, the experimental results have shown that the design from this thesis performs more responsive.

Keywords: Voice over IP software package; VoIP security; VoIP signaling protocol; SIP Flooding Attack

สารบัญ

หน้า

สารบัญตาราง

สารบัญรูป

หน้า

หน้า

บทที่ 1

บทนำ

1.1 หลักการและเหตุผล

การนำเทคโนโลยี Voice over IP (VoIP) มาใช้งานในปัจจุบันส่งผลให้เกิดประโยชน์ในเรื่องการลดค่าใช้จ่ายในการโทรศัพท์ และลดต้นทนขององค์กรได้อย่างมาก โดยเฉพาะซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพี (VoIP Open-source Software) ก็ได้เป็นที่นิยมของนักพัฒนาด้วยเหตุผลที่ไม่ต้องเสียค่าใช้จ่ายในเรื่องของลิขสิทธิ์และความยืดหยุ่นในการปรับแต่งใช้งาน ดังนั้นซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพี จึงเป็นที่นิยมสำหรับการนำมาพัฒนาต่อยอดประยุกต์ใช้งานกับองค์กรและหน่วยงานต่างๆ ในปัจจุบันมีซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพีที่เป็นที่นิยมนำมาใช้งานเช่น Asterisk [1], FreeSWITCH [2] และ Kamailo [3] เป็นต้น

ซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพียังมี มีความเสี่ยงด้านความมั่นคงอยู่มาก เช่น การดักฟังเสียงสนทนาด้วยเทคนิค Man in the Middle Attack (MITM) [4] การโจมตีเครื่องให้บริการ VoIP ปฏิเสธการให้บริการหรือ SIP Flooding [5, 6] ซึ่งปัญหาเหล่านี้จะทำเกิดความเสียหายต่อองค์กรเป็นอย่างมาก ซึ่งก็มีผู้นำเอาซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพีมาพัฒนาเป็นชุดซอฟต์แวร์และปรับปรุงประสิทธิภาพด้านความมั่นคงเช่น ISANBox.A [7] ที่สามารถป้องกันปัญหาด้านความมั่นคงดังกล่าวได้ และยังมีชุดซอฟต์แวร์อื่นๆ อีก เช่น EZY IP-PBX [8] AsteriskNOW for Thai [9] ซึ่งชุดซอฟต์แวร์ที่กล่าวมานั้นล้วนแต่พัฒนาขึ้นมากจาก Asterisk จากการศึกษาเรื่องการใช้งาน VoIP ปรากฏว่ามีรายงานจากเครือข่ายผู้ใช้งานซอฟต์แวร์ FreeSWITCH จากทั่วโลก [2, 10, 11] พบว่า FreeSWITCH มีประสิทธิภาพในด้านการรองรับคู่สาย ณ เวลาเดียวกัน (Concurrent Call) และความมีเสถียรภาพในการทำงานดีกว่า Asterisk อีกทั้งยังมีหลายบทวิเคราะห์ของกลุ่มผู้ดูแลระบบบนอินเทอร์เน็ตที่กล่าวถึง FreeSWITCH มีแนวโน้มประสิทธิภาพด้านคุณภาพการให้บริการในระดับที่แต่ก็พบว่าในประเทศไทย FreeSWITCH ยังไม่เป็นที่นิยมนำมาประยุกต์ใช้งานเป็นระบบ VoIP กันอย่างแพร่หลาย

อีกทั้งในปัจจุบันได้มีแนวทางแก้ไขปัญหาด้านความมั่นคงในระดับ Signaling Protocol โดยเฉพาะการแก้ไขปัญหา SIP Flooding ที่หลากหลายเช่นในงานวิจัยของ คธาวุฒิ จันบัวลา และสมนึก พ่วงพรพิทักษ์ [7] ได้เสนอวิธีการแก้ไขปัญหาโดยใช้เทคนิคการวิเคราะห์ไฟล์ Log ของระบบเพื่อตรวจจับการโจมตี อย่างไรก็ตามในงานวิจัยการแก้ไขปัญหา SIP Flooding ด้วยการอ่านไฟล์ Log นี้ ยังพบความไม่สมบูรณ์ของการป้องกัน คือการตอบสนองไม่ทันต่อเหตุการณ์การโจมตี ซึ่งส่งผลให้มีบางช่วงเวลาที่ไม่สามารถตรวจจับและป้องกันการโจมตีได้อย่างสมบูรณ์และทำให้ระบบ VoIP ล้มเหลวลงได้ ซึ่งถ้าหากระบบ VoIP ที่แก้ปัญหาด้วยการอ่านไฟล์ Log ถูกนำไปใช้ในทางธุรกิจที่มีความวิกฤติในการติดต่อสื่อสารสูง หรือธุรกิจที่มีความเข้มงวดในเรื่องความเสถียรของระบบ ก็อาจจะเกิดความเสียหายให้กับองค์กรหรือธุรกิจนั้นได้

และจากอีกหลายงสนวิจัย [12-15] แสดงให้เห็นว่าการนำเอาแนวทางแก้ไขปัญหาด้วยการเข้ารหัสข้อมูลเสียงมาใช้ส่งผลให้เกิด Overhead ในการเข้ารหัสและถอดรหัส จึงทำให้ซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านอินเทอร์เน็ตที่แก้ไขปัญหาด้านความมั่นคง จะมีปัญหาเรื่องคุณภาพการให้บริการที่ลดลงนั่นคือทำให้คุณภาพของเสียงลดลงและส่งผลต่อความพึงพอใจของผู้ใช้บริการ

ด้วยเหตุปัจจัยข้างต้นวิทยานิพนธ์นี้จึงเสนอการปรับปรุงประสิทธิภาพด้านความมั่นคงของซอฟต์แวร์ FreeSWITCH ทดสอบประสิทธิภาพด้านความมั่นคง และคุณภาพการให้บริการว่าเป็นไปตามที่มาตรฐานกำหนดไว้หรือไม่ อีกทั้งได้เสนอแนวคิดการปรับปรุงวิธีการแก้ไขปัญหา SIP Flooding โดยการปรับแก้ที่โพรโทคอล SIP ให้มีคุณสมบัติในการตรวจจับการโจมตีและตอบสนองต่อการโจมตีได้ดียิ่งขึ้น

1.2 วัตถุประสงค์ของการวิจัย

1) เพื่อปรับปรุงประสิทธิภาพด้านความมั่นคง ของซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพี

2) เพื่อออกแบบแนวทางแก้ไขปัญหา SIP Flooding โดยการปรับแก้ที่โพรโทคอล SIP

1.3 ความสำคัญของการวิจัย

1) ได้ชุดซอฟต์แวร์สำหรับโทรศัพท์ผ่านเครือข่ายไอพีที่มีความมั่นคง และได้ทราบถึงสารสนเทศด้านคุณภาพการให้บริการของชุดซอฟต์แวร์สำหรับโทรศัพท์ผ่านเครือข่ายไอพี

2) ได้แนวทางแก้ไขปัญหา วิธีการตรวจจับและป้องกันการโจมตี SIP Flooding ที่ตอบสนองต่อการโจมตีได้เร็วขึ้น สามารถออกรายงานการโจมตี แจ้งเตือนไปยังผู้ดูแลระบบได้

3) ได้ต้นแบบซอฟต์แวร์ที่สามารถนำไปผลิตในเชิงพาณิชย์ต่อไปได้ ซึ่งจะกระตุ้นให้เกิดการเจริญเติบโตของเศรษฐกิจไทยในด้านอุตสาหกรรมซอฟต์แวร์ของประเทศ

4) ช่วยลดค่าใช้จ่ายด้านการโทรศัพท์ขององค์กรต่างๆ โดยสามารถนำไปพัฒนาต่อยอดใช้ในหน่วยงานต่างๆ ของรัฐ เช่น โรงเรียน มหาวิทยาลัย ลดการนำเข้าซอฟต์แวร์จากต่างประเทศขององค์กร โดยประยุกต์ใช้ซอฟต์แวร์โอเพนซอร์ซที่พัฒนาต่อยอดให้มีความมันคงมั่นคงต่อการถูกจู่โจมและเป็นการสร้างภูมิคุ้มกันให้กับเศรษฐกิจจากการต้องพึ่งพาซอฟต์แวร์ราคาแพงจากต่างประเทศ

1.4 ขอบเขตของการวิจัย

1) ซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพีที่พัฒนาต่อยอดและปรับปรุงด้านความมั่นคงคือ FreeSWITCH

2) ปรับปรุงแก้ไขปัญหาด้านความมั่นคงของซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพี โดย มุ่งแก้ไขปัญหาการโจมตีดักฟังเสียง ปัญหาการโจมตี SIP Flooding และป้องกัน Session Hijacking

3) ทดสอบวัดคุณภาพการให้บริการของซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพี โดยใช้วิธีการ E-Model ตามมาตรฐาน ITU-T G.107

4) งานวิจัยมุ่งเน้นการออกแบบแนวทางแก้ไขปัญหาการโจมตีแบบ SIP Flooding ในรูปแบบที่ตอบสนองได้ทันต่อการโจมตี โดยการปรับแก้ที่โพรโทคอล SIP เท่านั้น

5) ออกแบบและพัฒนาโปรแกรมต้นแบบตามแนวทางเพื่อใช้แก้ไขปัญหา SIP Flooding โดยใช้ Jain-SIP API ภาษา Java

6) ค่าขีดแบ่ง (Threshold) ที่ใช้จำแนกรูปแบบการโจมตี SIP Flooding เลือกใช้แบบคงที่ที่เหมาะสมกับบริบทของเครือข่ายทดลองเท่านั้น โดยไม่ได้พิจารณาถึงค่าขีดแบ่งที่เหมาะสมในบริบทของเครือข่ายอื่นๆ

7) การทดลอง การออกแบบพัฒนาปรับปรุงประสิทธิภาพด้านความมั่นคง และการทดสอบคุณภาพการให้บริการ จะทำบนเครือข่ายทดสอบ (Test-beds) เท่านั้น

1.5 นิยามศัพท์เฉพาะ

1) ซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพี (VoIP Open-source Software) หมายถึง ซอฟต์แวร์ที่ทำหน้าที่เป็น VoIP Server ให้บริการสร้างและสิ้นสุดการเชื่อมต่อ จัดการคู่สายหมายเลขไอพี จัดการบัญชีผู้ใช้งาน เป็นซอฟต์แวร์ที่ไม่มีค่าใช้จ่ายเรื่องของลิขสิทธิ์ สามารถนำมาพัฒนาปรับแต่งแก้ไข Source Code ได้และเป็นที่นิยมใช้งานอย่างแพร่หลายเพราะมีความยืดหยุ่นสูง เช่น Asterisk, FreeSWITCH และ Kamailo เป็นต้น

2) Secure Real time Transport Protocol (SRTP) คือ โพรโทคอลที่ใช้เข้ารหัสและถอดรหัสข้อมูลแบบ Real time ก่อนส่งข้อมูลไปในเครือข่ายเพื่อรักษาความลับของข้อมูลนั้นๆ

3) คุณภาพการให้บริการการ (Quality of Service) หมายถึง ผลกระทบสะสมของสมรรถนะของการให้บริการการสื่อสารประเภทเสียงในเครือข่ายอินเทอร์เน็ต ซึ่งเป็นตัวกำหนดระดับของความพึงพอใจของผู้ใช้บริการตามข้อเสนอแนะ ITU-T E800

4) โพรโทคอลสัญญาณ (Signaling Protocol) คือโพรโทคอลที่ใช้ในการกำหนดข้อตกลงในการติดต่อสื่อสาร ถูกนำมาใช้ใช้สร้าง แก้ไข และสิ้นสุดเซสชันในการติดต่อสื่อสารในระบบ VoIP ตัวอย่าง เช่น โพรโทคอล Session Initiation Protocol (SIP)

5) SIP Flooding Attack คือเทคนิควิธีการโจมตีระบบ VoIP ที่มีจุดประสงค์เพื่อทำให้ระบบ VoIP เกิดการปฏิเสธการให้บริการกับผู้ใช้ทั่วไปซึ่งเป็นการโจมตีที่มีสถิติการเกิดขึ้นบ่อยกว่าการโจมตีแบบอื่นๆ โดยมีลักษณะการส่งแพ็กเก็ต Invite มายังระบบ VoIP เป็นจำนวนมากและในอัตราที่เร็วผิดปกติ จนทำให้ระบบ VoIP นั้นปฏิเสธการให้บริการในที่สุด

บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ในการศึกษาวิจัยในครั้งนี้ผู้วิจัยได้ทำการศึกษาทบทวนวรรณกรรมงานวิจัยและทฤษฎีต่างๆ ที่เกี่ยวข้องดังต่อไปนี้

2.1 ระบบโทรศัพท์ผ่านอินเทอร์เน็ต

ระบบโทรศัพท์อินเทอร์เน็ตหรือ Voice over Internet Protocol (VoIP) [16] คือเทคโนโลยีการสื่อสารด้วยเสียงผ่านเครือข่ายอินเทอร์เน็ต โดยผ่านการเข้ารหัสสัญญาณเสียง การเข้ารหัสสัญญาณเสียงสามารถทำได้หลายวิธี โดยแต่ละวิธีให้คุณภาพเสียง อัตราข้อมูล และการล่าช้าเวลาในการเข้ารหัสที่แตกต่างกัน ซึ่งคุณลักษณะทั้งหมดนี้เป็นปัจจัยที่สำคัญ และมีผลต่อคุณภาพของเสียง และคุณภาพของการให้บริการดังแสดงในตารางที่ 2.1

ตารางที่ 2.1 เปรียบเทียบคุณลักษณะของการเข้ารหัสสัญญาณเสียงแบบต่างๆ

Voice CODEC	Bit Rate (kbps)	CODEC Delay (ms)	Mean Opinion Score (MOS)
G.711 PCM	64	0.125	4.3-4.4
G.726 ADPCM	32	1	4.0-4.2
G.729 CS-ACELP	8	15	4.0-4.2
G.723.1 ACELP	5.3-6.4	37.5	3.5-4.0

ที่มา: [17]

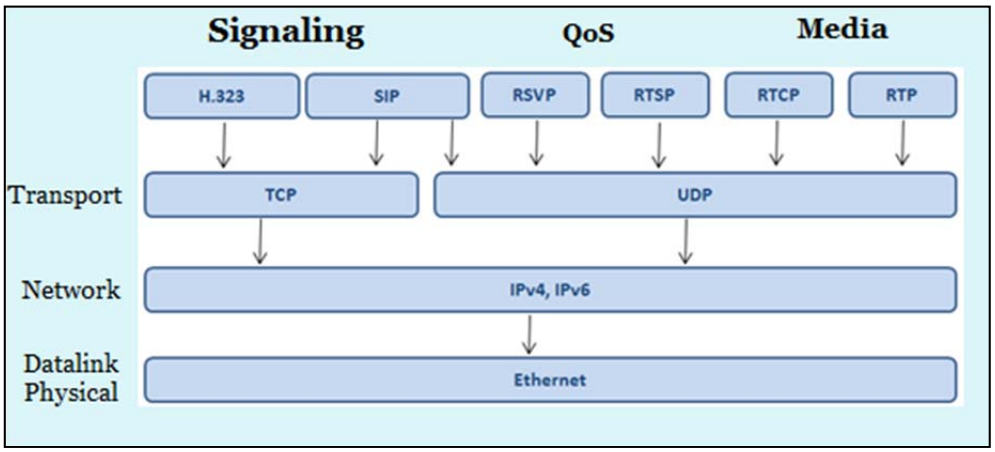
เนื่องจากการให้บริการเสียงเป็นการให้บริการที่ต้องการคุณสมบัติเวลาจริง และข้อมูลเสียงสามารถทนต่อการเกิดข้อมูลสูญหายบางส่วนได้ ดังนั้นการส่งข้อมูลเสียงผ่านโครงข่ายอินเทอร์เน็ตจึงใช้โพรโทคอล User Datagram Protocol (UDP) ซึ่งเป็นโพรโทคอลที่มีขนาดเล็ก และไม่รับประกันการสูญหายของข้อมูลแทนโพรโทคอล Transport Control Protocol (TCP) ซึ่งใช้รับประกันความถูกต้องของการรับส่งข้อมูล และมีความซับซ้อน ทำให้ไม่เหมาะสำหรับข้อมูลที่ต้องการคุณสมบัติแบบเวลาจริง (Real time) แต่เนื่องจากโพรโทคอล UDP นั้นไม่รับประกันการเรียงลำดับข้อมูลที่ได้รับที่ปลายทาง ดังนั้นจึงต้องใช้โพรโทคอล Real time Transport Protocol (RTP) มาควบคุมการเรียงลำดับแพ็กเก็ตข้อมูลเสียของโพรโทคอล UDP อีกทีแสดงโครงสร้างแพ็กเก็ตข้อมูลเสียงในรูปที่ 2.1

Eth/PPP Hdr (26 or 8 Bytes)	IP Hdr (20 Bytes)	UDP Hdr (8 Bytes)	RTP Hdr (12 Bytes)	Voice Sample	FEC/Filler (6 Bytes)

รูปที่ 2.1 โครงสร้างแพ็กเก็ตเสียงที่ส่งผ่านเครือข่าย

2.2 โพรโทคอลสัญญาณ (Signaling Protocol)

การสื่อสารข้อมูลเสียงระหว่างต้นทางกับปลายทางในระบบโทรศัพท์บนโครงข่ายอินเทอร์เน็ตนั้น จำเป็นต้องใช้โพรโทคอลสัญญาณเพื่อควบคุมการสร้าง การเปลี่ยนแปลง และการสิ้นสุดเซสชั่นการสื่อสารระหว่างต้นทาง กับปลายทาง ซึ่งในปัจจุบันมีโพรโทคอลสัญญาณสำหรับระบบโทรศัพท์อินเทอร์เน็ตที่นิยมใช้อยู่ 3 โพรโทคอลด้วยกันคือ H.323 [18], Session Initiation Protocol (SIP) [19] และ Skinny Client Control Protocol (SCCP) [20] แต่เนื่องจาก SIP ถูกพัฒนาขึ้นภายหลังและมีแนวทางในการพัฒนาขึ้นเพื่อรองรับการทำงานบนโครงข่ายอินเทอร์เน็ตโดยตรง โพรโทคอล SIP จึงเป็นที่นิยม มีความซับซ้อนน้อย สามารถปรับแต่งเพิ่มเติมคุณลักษณะของโพรโทคอลได้ง่าย สามารถรองรับการทำงานได้ทั้งในโพรโทคอล TCP และ UDP และสามารถทำงานบนโครงข่ายขนาดใหญ่ได้ดีกว่าเมื่อเปรียบเทียบกับโพรโทคอล H.323 ซึ่งโพรโทคอล SIP เป็นที่นิยมนำมาพัฒนาใช้งานโดยเฉพาะกับระบบ VoIP ดังแสดงโครงสร้างโพรโทคอลที่เกี่ยวข้องกับ VoIP ในรูปที่ 2.2 สุดท้ายคือโพรโทคอล SCCP ซึ่งเป็นโพรโทคอลที่ถูกพัฒนาให้รองรับการทำงานกับอุปกรณ์ของ Cisco เท่านั้น โดยโพรโทคอลนี้ถูกออกแบบพัฒนาในเชิงพานิชย์ ดังนั้นในการพัฒนาต่อยอดจึงไม่เป็นที่นิยมของกลุ่มนักพัฒนา

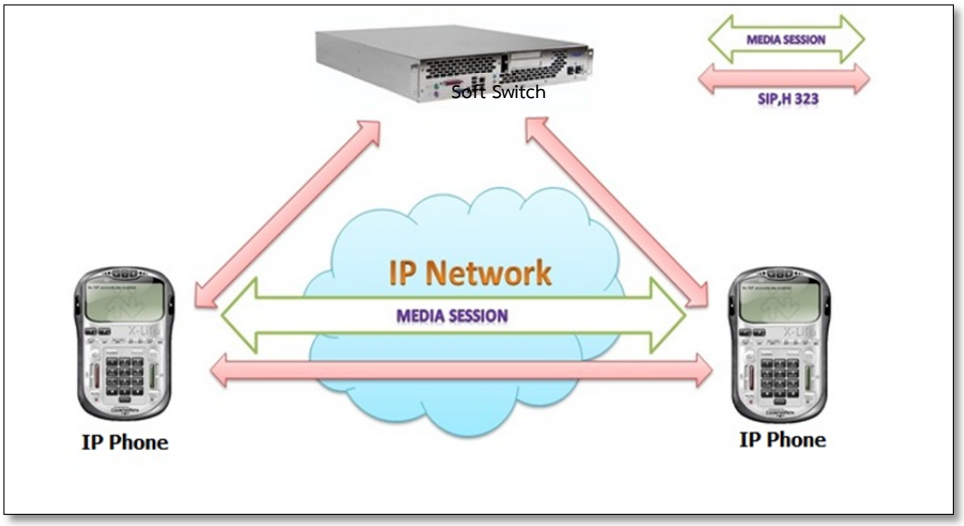


รูปที่ 2.2 โครงสร้างโพรโทคอลสำหรับระบบโทรศัพท์บนโครงข่ายอินเทอร์เน็ต

การอ้างอิงที่อยู่ของโครงข่ายอินเทอร์เน็ตนั้นใช้ไอพีแอดเดรส แต่สำหรับระบบโทรศัพท์การใช้ไอพีแอดเดรส เป็นตัวระบุเครื่องลูกข่ายของผู้ใช้โทรศัพท์นั้นไม่เหมาะสม เนื่องจากในการเชื่อมต่อโครงข่ายอินเทอร์เน็ตแต่ละครั้ง เครื่องลูกข่ายอาจได้ไอพีแอดเดรสที่ไม่เหมือนเดิม ดังนั้นจึงต้องมีแอดเดรสที่ใช้ระบุเครื่องลูกข่ายสำหรับการใช้งานโทรศัพท์อินเทอร์เน็ตโดยตรง ซึ่งในการใช้งานจริง

ภายในโครงข่ายต้องมี VoIP Server ทำงานเป็น Server จัดการจับคู่ไอพีแอดเดรส กับแอดเดรสสำหรับระบบโทรศัพท์ของเครื่องลูกข่ายแต่ละเครื่อง และช่วยควบคุมเซสชั่นระหว่างต้นทางกับปลายทาง ดังแสดงในรูปที่ 2.3 เมื่อผู้ใช้งานเข้าใช้ระบบ เครื่องลูกข่ายของระบบ โทรศัพท์อินเทอร์เน็ตจะลงทะเบียนกับ VoIP Server ก่อนโดยใช้ Signaling Protocol เช่น SIP หรือ H.323 เมื่อ VoIP Server ได้รับการร้องขอลงทะเบียนจากเครื่องลูกข่าย VoIP Server จะเก็บข้อมูลไอพีแอดเดรส และแอดเดรสสำหรับระบบโทรศัพท์ของเครื่องลูกข่ายไว้ ดังนั้น VoIP Server จะมีข้อมูลของเครื่องลูกข่ายทุกเครื่องที่ได้เข้ามาลงทะเบียนไว้

สำหรับโทรศัพท์อินเทอร์เน็ตปลายทาง เครื่องลูกข่ายต้นทางจะส่งข้อความร้องขอไปยัง VoIP Server โดยใช้ Signaling Protocol SIP หรือ H.323 เมื่อ VoIP Server ได้รับข้อความร้องขอจากเครื่องลูกข่ายต้นทาง VoIP Server จะตรวจสอบแอดเดรสปลายทาง พร้อมกับค้นหาไอพีแอดเดรสของเครื่องลูกข่ายปลายทางจากฐานข้อมูล และส่งข้อความร้องขอนั้นต่อไปยังเครื่องลูกข่ายปลายทางตามไอพีแอดเดรสที่ได้ลงทะเบียนไว้ หรืออาจส่งไอพีแอดเดรสของเครื่องลูกข่ายปลายทางกลับไปให้เครื่องลูกข่ายต้นทางทราบเพื่อใช้ในการติดต่อต่อไป เมื่อเครื่องลูกข่ายทั้ง 2 ทราบไอพีแอดเดรสของกันและกันแล้ว ก็จะสามารถส่งสัญญาณ รวมไปถึงข้อมูลเสียงหากันได้โดยตรง ทั้งนี้จะเห็นได้ว่า VoIP Server เป็นอุปกรณ์ที่ประมวลผลสัญญาณ เพื่อช่วยสร้างเซสชั่นในระบบโทรศัพท์อินเทอร์เน็ตเท่านั้น โดยข้อมูลเสียงไม่จำเป็นต้องวิ่งเข้าไปที่ VoIP Server



รูปที่ 2.3 การส่ง Signaling และ Media ผ่านโครงข่ายอินเทอร์เน็ต

2.2.1 ขั้นตอนการทำงานของโพรโทคอล SIP

การทำงานของโพรโทคอล SIP ในระบบ VoIP มีกระบวนการและขั้นตอนการทำงานโดยมีรายละเอียดดังต่อไปนี้

1) Call Setup

Call Setup เป็นการเริ่มต้นการติดต่อ โดยผู้ร้องขอการติดต่อทำการติดต่อไปยังผู้ถูกร้องขอการติดต่อครั้งแรกเพื่อเรียกร้องการสนทนา ในส่วนนี้ จะใช้ SIP Message ที่ชื่อว่า Message INVITE ทำการร้องขอการติดต่อไปยังปลายทาง

2) Media & Channel Control

Media & Channel Control เป็นการตกลงหรือทำการระบุข้อตกลงต่างๆ ที่ต้องใช้ในการส่งข้อมูลเสียง ได้แก่ มาตรฐานการบีบอัดข้อมูลเสียง หมายเลข IP Address และหมายเลข Port เป็นต้น โดยในส่วนนี้ จะนำโพรโทคอล Session Description Protocol (SDP) มาช่วยในการตกลงรูปแบบการติดต่อนี้

3) Media Stream

Media Stream เป็นขั้นตอนของการส่งข้อมูลเสียงโดยใช้ตามข้อตกลงที่ได้ตกลงกันในขั้นตอนที่ 2 Media & Channel Control โดยทั่วไปจะนิยมใช้ Real-Time Transport Protocol (RTP) ในการส่งข้อมูลเสียงในขั้นตอนนี้ ซึ่งขั้นตอนนี้ไม่ได้อยู่ในความรับผิดชอบของโพรโทคอล SIP

4) End Call

End Call เป็นขั้นตอนการส่งสัญญาณระหว่างผู้ร้องขอการติดต่อและผู้ถูกร้องขอการติดต่อเพื่อขอจบการติดต่อ โดยในส่วนนี้จะใช้ SIP Message ที่ชื่อว่า Message BYE เป็นสัญญาณในการสิ้นสุดการติดต่อ หลังจากจบขั้นตอนนี้ช่องทางของสัญญาณที่สร้างขึ้นทั้งหมดจะถูกปิด หากต้องการเริ่มสนทนาใหม่ จะต้องทำการติดต่อตามขั้นตอนเริ่มตั้งแต่ Call Setup ใหม่ทั้งหมด

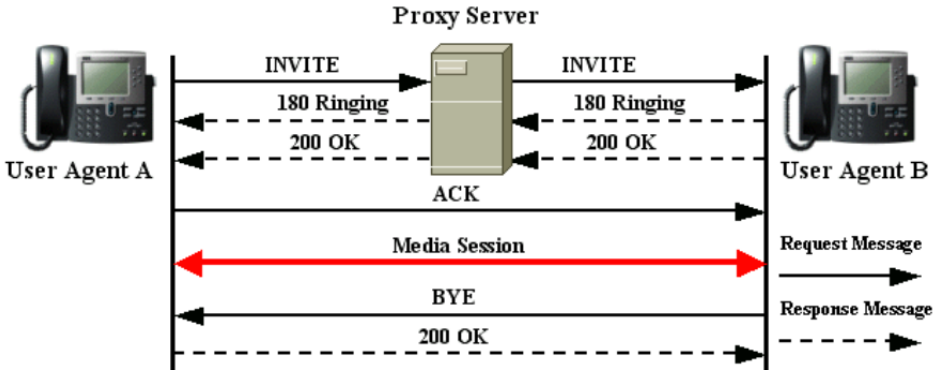
2.2.2 ลักษณะการทำงานของ SIP Server

โดยได้มีการแบ่งรูปแบบการทำงานของ SIP Server ที่ใช้สำหรับระบบ VoIP โดยได้แบ่งตามลักษณะการทำงานของโพรโทคอล SIP ได้ 3 รูปแบบดังนี้

1) Proxy Server

Proxy Server เป็น SIP Server ที่ทำหน้าที่เป็นตัวกลางในการติดต่อระหว่างผู้ร้องขอการติดต่อและผู้ถูกร้องขอการติดต่อ โดยการทำงานในขั้นตอน Call Setup, Media & Channel Control และ End Call การส่งสัญญาณทุกอย่างในขั้นตอนทั้งหมดนี้จะต้องทำผ่าน SIP Server โดย SIP Server จะทำการตรวจสอบ SIP Message ที่ได้รับทุกครั้งและจะทำการส่ง SIP Message นั้นไปยังปลายทางที่ต้องการ โดยอาจมีการเปลี่ยนแปลงรูปแบบของ SIP Message ตามความเหมาะสม สำหรับการทำงานในขั้นตอนการส่งข้อมูลเสียง (Media Stream) จะไม่ผ่าน SIP Server นั่นคือ SIP Client ทั้ง 2 ฝ่ายจะทำการส่งข้อมูลเสียงกันโดยตรง เมื่อมองในระดับ Logical แต่หากมองในระดับ Physical แล้ว SIP Client ทั้ง 2 ฝ่ายอาจมีการส่งข้อมูลผ่าน Server หรือ Gateway ก็ได้ เนื่องจากการทำงานทั้งหมดมีพื้นฐานการทำงานอยู่บนระบบเครือข่าย Internet ดังนั้นการส่งข้อมูลสามารถส่งผ่านแต่ละโหนด (Node) เพื่อให้สามารถส่งข้อมูลไปยังปลายทางที่ต้องการได้ ดังจะเห็นได้ว่า Proxy Server จะทำหน้าที่รับผิดชอบการติดต่อระหว่างผู้ร้องขอการติดต่อและผู้ถูกร้องขอการติดต่อ ทำให้ Proxy Server สามารถทำการเพิ่มเติมความสามารถต่างๆ เพื่อให้สามารถให้บริการ SIP Client ได้ดียิ่งขึ้น แต่อย่างไรก็ตามการทำงานในลักษณะนี้ทำให้ต้องสูญเสียเวลาในช่วงการติดต่อที่ทำโดยตัว Proxy Server และ Proxy Server สามารถให้บริการ SIP Client ได้จำกัดขึ้นอยู่กับความสามารถของ Proxy Server นั้นๆ ที่จะสามารถรองรับการบริการกับ SIP Client ที่ทำการติดต่อ

ได้มากน้อยเพียงไรโดยเห็นได้จากรูปที่ 2.4 เป็นการแสดงให้เห็นถึงการสร้างและสิ้นสุดเซสชั่นโดยผ่านเครื่องแม่ข่าย



ที่มา: [17]

รูปที่ 2.4 การสร้างและสิ้นสุดเซสชั่นโดยผ่านเครื่องแม่ข่าย Proxy

2) Registrar Server

Registrar Server เป็น SIP Server ที่ทำหน้าที่ในการรับการลงทะเบียนจาก SIP Client โดยจะทำการเก็บข้อมูลทั้งหมดไว้ใน Location Server ซึ่งโดยทั่วไป Registrar Server ก็คือ SIP Sever เมื่อทำหน้าที่รับการลงทะเบียนนั่นเอง เมื่อผู้ร้องขอการติดต่อทำการส่ง Request Message ไปยัง SIP Registrar Server ตัว SIP Registrar Server จะทำการติดต่อไปยัง Location Service ของ Location Server เพื่อถามหาที่อยู่ของผู้ถูกร้องขอการติดต่อโดยสัญญาณที่ใช้นี้ตามมาตรฐานของ SIP ไม่มีการกำหนดไว้ ดังนั้น SIP Registrar Server สามารถกำหนดรูปแบบของสัญญาณที่ใช้ติดต่อระหว่าง SIP Registrar Server กับ Location Server ได้เอง ต่อมาเมื่อ Location Server สามารถหาที่อยู่ได้แล้วก็จะส่งมาบอกกับ SIP Registrar Server สุดท้าย SIP Registrar Server จะส่ง Response Message ไปให้ผู้ร้องขอการติดต่อเพื่อบอกที่อยู่ของผู้ถูกร้องขอการติดต่อตามที่ผู้ร้องขอการติดต่อต้องการ

3) Redirect Server

Redirect Server เป็น SIP Server ที่ทำหน้าที่ในการระบุที่อยู่ของผู้รับการติดต่อที่ได้ทำการลงทะเบียนไว้ โดยจะทำการหาที่อยู่จาก Location Server ซึ่งเมื่อหาที่อยู่ได้แล้วจะส่งที่อยู่ทั้งหมดที่หาได้ให้กับผู้ร้องขอการติดต่อ ดังนั้นหลังจากที่ SIP Client ได้ที่อยู่ในการติดต่อแล้วจะต้องทำการติดต่อไปยังปลายทางที่ต้องการตามที่อยู่ที่ได้นั้นเอง โดยหากผู้ร้องขอการติดต่อได้ที่อยู่มากกว่า 1 ที่อยู่ ผู้ร้องขอการติดต่อจะต้องทำการติดต่อไปยังทุกๆที่อยู่เพื่อหาที่อยู่จริงๆ ของผู้ถูกร้องขอการติดต่อเอง ดังจะเห็นได้ว่าการทำงานในลักษณะนี้จะทำให้ภาระในการติดต่อทั้งหมดตกอยู่ที่ตัว SIP Client แต่การทำงานลักษณะนี้จะทำให้ SIP Client สามารถทำการติดต่อได้อย่างรวดเร็วในกรณีที่ได้ที่อยู่เดียวจาก SIP Server และตัว SIP Server สามารถให้บริการกับ SIP Client ได้จำนวนมาก ซึ่งแสดงคุณสมบัติที่แตกต่างกันระหว่าง Proxy Server และ Redirect Server ในตารางที่ 2.2 [17]

ตารางที่ 2.2 คุณสมบัติของ Proxy Server และ Redirect Server

Proxy Server	Redirect Server
ทำงานได้ทั้งแบบ Stateless และ Statefull	สามารถให้บริการกับ SIP Client ได้จำนวนมาก
มีความยืดหยุ่นในการทำงานสูง และ สามารถเพิ่มเติมการบริการได้ต้องการ	หน้าที่หรือความรับผิดชอบในการติดต่อจะขึ้นอยู่กับ SIP Client
รับผิดชอบในทุกขั้นตอนการติดต่อทั้งหมด	เสียงจะสื่อสารโดยตรงระหว่าง Client to Client
จำนวน SIP Client ที่สามารถให้บริการได้ขึ้นอยู่กับการแบ่งส่วนการทำงานของ SIP Server	ไม่สามารถจัดการ Media ได้โดยตรง (ไม่สามารถบันทึกการสนทนาได้)
อาจสร้างเป็น Hybrid (Semi-Stateful) เพื่อให้เกิดประโยชน์สูงสุดแก่ SIP Client	การดำเนินการใช้ Secure Real-time Transport Protocol จะขึ้นอยู่ที่ Client เป็นหลัก

2.3 Session Initiation Protocol (SIP)

โพรโทคอล SIP [19] ถูกพัฒนาขึ้นโดยคณะทำงาน IETF (Internet Engineering Task Force) มีวัตถุประสงค์เพื่อใช้ในการสร้าง เปลี่ยนแปลงแก้ไข และสิ้นสุดเซสชั่นบนเครือข่ายอินเทอร์เน็ต โดยที่โพรโทคอล SIP ถูกออกแบบมาให้ง่ายต่อการพัฒนาใช้งาน สะดวกต่อการเพิ่มเติม ปรับปรุงคุณสมบัติของโพรโทคอล และที่สำคัญคือสามารถนำโพรโทคอล SIP มาประยุกต์ใช้กับโครงข่ายขนาดใหญ่ได้เป็นอย่างดี โดยที่การทำงานของโพรโทคอล SIP จะมีการส่งข้อความเพื่อระบุการเจรจาตกลงการติดต่อสื่อสารโดยมีการกำหนดรูปแบบข้อความ 6 รูปแบบดังนี้

ข้อความ INVITE คือข้อความร้องขอที่มีการส่งเพื่อเชิญให้มีการติดต่อสื่อสารไปยังปลายทางให้เข้าร่วมอยู่ในเซสชั่นการติดต่อสื่อสารเดียวกัน โดยจะมีค่าพารามิเตอร์ต่างๆ ที่เก็บไว้ใน Message body ของเซสชั่นที่ผู้เรียกต้องการใช้ในการติดต่อ เมื่อปลายทางหรือผู้รับ ได้รับข้อความร้องขอ INVITE แล้ว จะส่งข้อความตอบสนองกลับไปยังต้นทางเพื่อตอบรับ หรือปฏิเสธการเรียกนั้น ในกรณีที่ตอบรับการร้องขอผู้รับจะระบุค่าพารามิเตอร์ต่างๆ ที่ผู้รับต้องการไว้ใน Message body ของข้อความตอบสนองนั้น

ข้อความ ACK คือข้อความร้องขอที่ใช้ในการยืนยันการตอบตกลงในการเชื่อมต่อถึงกัน ถูกใช้ในกรณี ผู้ใช้ได้รับข้อความตอบสนองสุดท้ายของการ้องขอ INVITE จากเครื่องแม่ข่ายเรียบร้อยแล้ว

ข้อความ BYE คือข้อความร้องขอที่ใช้ในการขอยกเลิกเซสชั่นการติดต่อ โดยทั้งต้นทางหรือปลายทางก็สามารถส่งข้อความร้องขอ BYE นี้ได้เช่นกัน

ข้อความ CANCEL คือข้อความร้องขอที่ใช้สำหรับบอกผู้รับปลายทางว่าผู้ส่งต้นทางต้องการยกเลิกข้อความร้องขอที่ได้ส่งไปก่อนหน้านี้และยังไม่ได้รับการตอบรับกลับมา

ข้อความ OPTIONS คือข้อความร้องขอที่ใช้บอกข้อมูลเพิ่มเติมเกี่ยวกับความสามารถ (Capability Information) ของเครื่องลูกข่ายให้เครื่องแม่ข่ายทราบ และใช้ในการสอบถามข้อมูลเกี่ยวกับเครื่องแม่ข่ายด้วย

ข้อความ REGISTER คือข้อความร้องขอที่ใช้สำหรับการขอลงทะเบียนระหว่างเครื่องลูกข่ายกับเครื่องแม่ข่าย

2.4 Real-Time Transport Protocol (RTP)

RTP [21] จะทำงานในลักษณะเครือข่าย End-to-End การทำงานของ RTP จะทำงานไม่คำนึงถึง Quality of Service (QoS) โดยใช้กับการส่งแบบเวลาจริง (Real time) ข้อมูลที่ส่งจะถูกจัดการโดย RTCP (Real Time Control Protocol) เพื่อที่จะส่งในระบบ Network RTP สามารถส่งข้อมูลได้แบบ Unicast และ Multicast RTP ถูกออกแบบมาโดยไม่ขึ้นกับ Transport และ Network layers สามารถใช้ในการส่งข้อมูลผ่านเครือข่ายสำหรับการส่งข้อมูลพวกใช้เวลาจริง (Real Time) เช่น ทางวีดีทัศน์ (Video) เสียง Audio แบบ Real Time ซึ่งไม่มีข้อกำหนดที่แน่นอนสามารถใช้ได้ทั้ง TCP และ UDP ซึ่งโดยทั่วไปจะใช้ UDP นอกจากนั้นยังไม่มีช่วงของ Port ที่แน่นอน ข้อมูลที่ส่งจะถูกควบคุมด้วย RTCP ซึ่ง RTP เป็นการเชื่อมต่อแบบ Connectionless ไม่มีการรับประกันคุณภาพของข้อมูลที่ส่ง หมายความว่าไม่ได้มีกลไกใดๆ ในการยืนยันข้อมูลว่าส่งได้สำเร็จหรือไม่ ซึ่งแตกต่างจากโพรโทคอล UDP เมื่อทำการส่งแล้วอาจมีปัญหาในการลำดับก่อนหลังของเฟรม

2.5 ซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพี (VoIP Open-source Software)

ซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพี คือ ซอฟต์แวร์ที่ทำหน้าที่เป็น VoIP Server ให้บริการสร้างและสิ้นสุดการเชื่อมต่อ จัดการคู่สาย หมายเลขไอพี จัดการบัญชีผู้ใช้งาน เป็นซอฟต์แวร์ที่ไม่มีค่าใช้จ่ายเรื่องของลิขสิทธิ์ สามารถนำมาพัฒนาปรับแต่งแก้ไข Source Code ได้และเป็นที่นิยมใช้งานอย่างแพร่หลายเพราะมีความยืดหยุ่นสูงและมีซอฟต์แวร์ที่กำลังได้รับความนิยม ดังนี้

2.5.1 Asterisk

Asterisk [1] คือ Open-source Software ที่ทำหน้าที่หลักเป็น IP-PBX หรือที่เรียกว่าตู้ชุมสายโทรศัพท์ระบบ IP ซึ่งมีหน้าที่ในการควบคุมและจัดการบริหาร การเชื่อมต่อทั้งยังสามรถเพิ่มเติมประสิทธิ์ภาพและความสามารถในการทำงานได้โดยง่าย Asterisk สามารถทำหน้าเป็นอุปกรณ์สลับสายโทรศัพท์ไม่ว่าจะเป็นระบบ IP หรือ Hybridge สามรถทำการตั้งค่าเส้นทางการของการโทรศัพท์โดยตัวเอง สามารถเพิ่มเติมฟังก์ชันได้เช่น ระบบ Voicemail, IVR, Call Center และรองรับการเชื่อมต่อกับระบบโทรศัพท์พื้นฐานไม่ว่าจะเป็นแบบ Analog หรือ Digital (ISDN) อีกทั้งยังสามารถทำหน้าที่เป็น Gateway เชื่อมต่อระหว่าระบบโทรศัพท์พื้นฐานกับระบบ VoIP โดยที่ Asterisk ได้รับความนิยมใช้งานอย่างแพร่หลายโดยเฉพาะกับหน่วยงานในประเทศไทยได้มีกลุ่มวิจัยภายในประเทศนำเอา Asterisk ไปพัฒนาเป็นชุดซอฟต์แวร์วีโอไอพี เช่น IP Communication Lab มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี ได้พัฒนาขึ้นเป็น EZY IP-PBX และ Information Security and Advance Network มหาวิทยาลัยมหาสารคาม ได้พัฒนาขึ้นเป็น ISAN Box.A เป็นต้น

FreeSWITCH

FreeSWITCH [2] คือ Software ที่ถูกพัฒนาขึ้นในปี ค.ศ. 2006 จากทีมผู้สร้าง Asterisk เดิมโดยการนำของ Anthony Minessale โดยเน้นแก้ปัญหาเรื่องประสิทธิภาพการใช้งานของ FreeSWITCH ทำหน้าที่ได้ทั้ง IP-PBX ในปัจจุบันยังมีการพัฒนาฟังก์ชันทำงานได้หลากหลายเท่า Asterisk แต่เนื่องด้วยการ Design ที่ใช้ XML ไฟล์ได้ดีกว่า Asterisk ทำให้รองรับการทำงานใช้คู่สาย ณ เวลาเดียวกัน (Concurrent Call) ได้มากกว่า Asterisk และยังมีความเสถียรมากกว่า รวมไปถึงยังมีความเป็น SIP Standard มากกว่า Asterisk เนื่องจากใช้ SIP Stack ของ Sofia และมีการใช้ SQLlite ในส่วนใหญ่ของการเก็บค่า Configure และการทำงานส่วนใหญ่ของระบบ และที่น่าสนใจคือการรองรับการทำงานร่วมกับ VoIP Protocol อื่นๆ สนับสนุนโพรโทคอล SRTP และ Secure SIP ซึ่งเป็นคุณสมบัติทางด้านความมั่นคง อีกทั้งยังพบหลายบทวิเคราะห์บนอินเทอร์เน็ตที่แสดงให้เห็นถึงคุณภาพการให้บริการของซอฟต์แวร์ FreeSWITCH ที่มีแนวโน้มอยู่ในระดับที่ดี และเป็นไปตามที่มาตรฐานกำหนดอีกด้วย

2.5.2 Kamailo

Kamailo [3] ชื่อเดิมคือ OpenSER เป็นซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพี ภายใต้ GPL ลองรับการเชื่อมต่อได้พร้อมๆ กันนับ 1000 การเชื่อมต่อ โดยสามารถใช้โพรโทคอลในการติดต่อสื่อสารได้ทั้ง TCP, UDP และ SCTP เป็นการสื่อสารที่มีความปลอดภัยผ่าน TLS สามารถใช้งานได้กับสื่อทั้งประเภทเสียงและวิดีโอ และใช้งานได้กับ IPv4 และ IPv6 มีระบบข้อความโต้ตอบแบบทันที IVR มีระบบจัดการและเส้นทางที่สั้นที่สุด มีระบบจัดการ Load Balancing, Routing Fail-Over, Accounting, Authentication และ Authorization ทำงานได้กับซอฟต์แวร์หลักหลายๆ อย่างเช่น MySQL, Postgres, Oracle, Radians และ LDAP Kamailo สามารถสร้างระบบ VoIP ขนาดใหญ่ได้ ยังสามารถเชื่อมต่อ SIP Gateway ไปยัง PSTN ได้ แต่จากงานวิจัย [4] และรายงานด้านความมั่นคง ของกลุ่มผู้ใช้ยังพบปัญหาเรื่องความมั่นคงอยู่มาก

2.6 ความมั่นคงปลอดภัยกับ Voice over Internet Protocol (VoIP)

การออกแบบระบบในการใช้งาน VoIP ประเด็นเรื่องความมั่นคงปลอดภัยของ VoIP มีหลักสำคัญที่ไม่ควรมองข้ามคือด้านความมั่นคงปลอดภัยซึ่งจะสามารถแบบออกเป็น 3 ส่วนดังนี้

2.6.1 ความสามารถของการให้บริการ

ความสามารถของการให้บริการของระบบเราจะต้องมั่นใจว่ารูปแบบการให้บริการของระบบนั้นตรงกับความต้องการ และระบบต้องมี Availability สูงพอกับความต้องการใช้งาน แอพพลิเคชันต่างๆ ที่เชื่อมต่อเข้ากับระบบ VoIP จะต้องพร้อมใช้งานได้ทันทีเมื่อต้องการ และจะต้องมีหน้าตาที่สะดวกต่อการใช้งานของผู้ใช้ มีโพรโทคอลสื่อสารที่แน่นอนควบคุมได้ง่าย หน่วยความจำของเครื่องซีพียู และแบนด์วิดธ์ของระบบต้องมีมากพอ รวมไปถึงแม้แต่การรองรับสำหรับปัญหาเนื่องจากซีพียูทำงานไม่ทันกับระบบจะต้องไม่เกิดขึ้นอีกด้วย

2.6.2 Service Integrity หรือระดับสิทธิในการใช้บริการ

Service Integrity หรือระดับสิทธิในการใช้บริการเป็นประเด็นค่อนข้างสำคัญสำหรับการป้องกันการใช้งานระบบโดยไม่ได้รับอนุญาต ซึ่งสิทธิทุกอย่างนั้นก็จะไปสัมพันธ์กับฟังก์ชันของระบบและข้อมูลในระบบด้วยเช่นกัน อย่างเช่นพนักงานฝ่ายการเงิน หรือฝ่ายบัญชีอาจจะไม่สามารถติดต่อ

ข้ามสำนักงานได้โดยตรง แต่ผู้จัดการฝ่ายสามารถติดต่อข้ามสาขาและข้ามประเทศได้ หรือพนักงานอาจจะติดต่อได้เฉพาะในเวลางานเท่านั้น เว้นแต่ฝ่ายบริการลูกค้า และระดับผู้บริหารเท่านั้นที่มีสิทธิในการใช้งานได้ตลอด 24 ชั่วโมง ตรงนี้ก็เพื่อรักษาสิทธิของบริษัทที่ป้องกันพนักงานนำระบบ VoIP ไปใช้โทรทางไกลข้ามประเทศในเรื่องส่วนตัวของพนักงานเอง ซึ่งอาจจะส่งผลให้องค์กรสูญเสียรายได้เป็นจำนวนมาก อีกทั้งยังเป็นการกำหนดสิทธิการเข้าถึงข้อมูลต่างๆ เพื่อควบคุมด้านความมั่นคงอีกด้วย

2.6.3 การรักษาความลับและความเป็นส่วนตัว

การรักษาความลับและความเป็นส่วนตัวเป็นประเด็นหลักที่ผู้ดูแลระบบส่วนใหญ่จะมองเป็นประเด็นแรกเสมอ เพราะเราจะต้องทำอย่างไรก็ได้ให้สัญญาณที่ส่งออกไปนั้นกลายเป็นความลับ หรือถ้าโดนดักจับจากระบบ (Sniffing) ก็จะต้องไม่สามารถถอดรหัสออกมาได้ ซึ่งเป็นกระบวนการทางด้านความมั่นคงที่ผู้ดูแลระบบต้องคำนึงถึง เช่นการใช้งานโพรโทคอล SRTP หรือ SIPS เป็นต้น แต่ไม่จำเป็นว่าจะต้องเป็นสัญญาณเพียงอย่างเดียว แม้แต่เสียงหรือการสื่อสารอื่นๆ ผ่านเว็บก็จะต้องรักษาความลับได้ดีไม่แพ้กัน และแม้แต่ข้อมูลส่วนตัวของลูกค้า หรือพนักงานก็จะหลุดออกไปจากระบบไม่ได้เลยเช่นกัน

2.7 ปัจจัยที่มีผลต่อคุณภาพการให้บริการของระบบ VoIP

คุณภาพการให้บริการ (Quality of Service) หรือคุณภาพของเสียงนั้นมีผลโดยตรงกับการออกแบบระบบ ซึ่งมาจาก 5 ปัจจัยประกอบด้วย ความสามารถในการให้บริการ (Availability) ทรูพุต (Throughput) ค่าหน่วงเวลาหรือค่าความล่าช้า (Latency or Delay) การผันผวนของค่าหน่วงเวลา (Delay Variation) และจำนวนแพ็กเก็ตที่สูญหาย (Packet Loss) [22] โดยมีรายละเอียดดังต่อไปนี้

2.7.1 ความพร้อมในการให้บริการ (Availability)

ความสามารถในการให้บริการคือความพร้อมที่เครือข่ายสามารถทำงานและให้บริการได้ โดยที่ความพร้อมในการให้บริการที่สูง สามารถทำได้โดยใช้อุปกรณ์ที่มีเสถียรภาพและเครือข่ายที่ไว้ใจได้ อย่างไรก็ตามการคำนวณความพร้อมในการให้บริการนี้ จะคิดโดยใช้หลักความน่าจะเป็น เพราะฉะนั้นการคำนวณโดยรวมค่า Mean Time Between Failure (MTBF) ของอุปกรณ์แต่ละตัวเข้าด้วยกันจึงไม่ใช่มาตรฐานวัดที่ถูกต้องนัก

2.7.2 ทรูพุต (Throughput)

ทรูพุต (Throughput) คือจำนวน Traffic ที่ถ่ายโอนในช่วงเวลาใด ๆ โดยปกติแล้วการสนทนาบนระบบแลน ถ้ามี Bandwidth มากเท่าใดคุณภาพก็จะดีตามไปด้วย หากเป็นระบบแวนซึ่งมีความเร็วของจุดเชื่อมต่อจำกัดแล้ว ทรูพุตจะขึ้นอยู่กับจำนวนเงินที่จ่ายให้กับการเช่าคู่สาย ดังนั้นองค์กรจำเป็นต้องคำนวณประสิทธิภาพการบีบอัดข้อมูลและการจำกัด Bandwidth ที่เหมาะสมเพื่อให้การสื่อสารด้วยเสียงมีคุณภาพดีพอ ในขณะที่ไม่เสียค่าใช้จ่ายมากเกินไป ทั้งนี้ก็ขึ้นอยู่กับการบริหารจัดการระบบ VoIP ให้มีประสิทธิภาพด้านคุณภาพการให้บริการที่ดีที่สุด

2.7.3 ค่าหน่วงเวลา (Delay)

จะคำนวณโดยใช้ค่าเฉลี่ยของเวลาที่ข้อมูลเข้าจนถึงออกจากเครือข่ายเซอร์วิสหลายอย่าง โดยเฉพาะอย่างยิ่งการสื่อสารด้วยเสียง ค่าหน่วงเวลานับว่ามีผลอย่างมากต่อคุณภาพ เพราะ

ถ้าค่าหน่วงเวลาอยู่ระหว่าง 100 ถึง 150 มิลลิวินาที ก็จะทำให้การสนทนาระหว่างผู้ใช้ไม่เป็นธรรมชาติ ในขณะที่ถ้ามากกว่า 200 มิลลิวินาที ก็จะทำให้การสื่อสารเกิดความยากลำบาก ซึ่งถ้าต้องการให้คุณภาพของเสียงดีพอนั้น ระบบเครือข่ายจำเป็นต้องมีค่าหน่วงเวลาที่ไม่มากเกินไปโดย ITU-T G.114 แนะนำว่าค่าหน่วงเวลาไปกลับ (Round Trip Delay) ของการสื่อสารด้วยเสียงระหว่างเกตเวย์ของ VoIP นั้นไม่ควรมากกว่า 300 มิลลิวินาที หรือคิดเป็น 150 มิลลิวินาที ในการส่งข้อมูลทางเดียว โดยค่าหน่วงเวลาของการสื่อสารนั้นเกิดขึ้นจากหลายสาเหตุ เช่น ความหนาแน่นของทราฟฟิก ความไม่เสถียรของอุปกรณ์เครือข่าย เป็นต้น

2.7.4 ค่าหน่วงเวลาของแพ็กเก็ตข้อมูล (Packet Delay)

ค่าหน่วงเวลาในการกระจายข้อมูล (Propagation Delay) เป็นเวลาที่ข้อมูลใช้ในการเดินทางผ่านเคเบิล (ทองแดง ไฟเบอร์ออปติกหรือคลื่นวิทยุ) ถึงแม้ว่าข้อมูลจะเดินทางผ่านสื่อเหล่านี้ด้วยความเร็วที่ใกล้เคียงกับความเร็วของแสง ซึ่งเป็นค่าคงที่ก็ตาม แต่ถ้าแพ็กเก็ตต้องเดินทางอ้อมโดยไม่จำเป็น ค่าหน่วงเวลาที่เกิดขึ้นจากการกระจายข้อมูล ก็จะเพิ่มขึ้นตามไปด้วย

เวลาในการเข้าคิว (Queuing Delay) เมื่อแพ็กเก็ตถูกส่งลงในเครือข่ายแล้ว ข้อมูลหลาย ๆ แหล่ง จำเป็นต้องเข้าคิวเพื่อถูกส่งไปบนเส้นทางเดียวกันซึ่งการเข้าคิวเพื่อรอรับการส่งนี้ก่อให้เกิดค่าหน่วงเวลาขึ้น สำหรับเทคโนโลยีบางอย่าง เช่น Asynchronous Transfer Mode (ATM) จึงพยายามลดค่าหน่วงเวลาในการเข้าคิว ด้วยการตัดแพ็กเก็ตต้นฉบับออกเป็นชิ้นเล็ก ๆ จากนั้นก็จับรวมกันเป็นเซลล์ แล้วส่งลงไปในคิวที่มีการจัดลำดับความสำคัญ (Priority Queue) ไว้แล้ว ด้วยขนาดของเซลล์ที่เล็ก ทำให้ข้อมูลในคิวที่มีความสำคัญมากกว่าจะถูกส่งบ่อยกว่า ซึ่งก็เท่ากับว่าเวลาที่คอยในคิวก็น้อยลงและสามารถคาดเดาได้ (Deterministic)

การผันผวนของค่าหน่วงเวลา เป็นมาตรวัดที่บ่งบอกความแตกต่างของค่าหน่วงเวลาในแต่ละแพ็กเก็ตข้อมูล เพราะถ้ามีความผันผวนมากจะเรียกว่า Jitter แต่ถ้าผันผวนน้อยจะเรียกว่า Wonder ค่าความผันผวนนี้จะมีผลต่อทราฟฟิกของการส่งข้อมูลแบบเรียลไทม์ เช่น วีดีโอคอนเฟอร์เรนซ์หรือโทรศัพท์ผ่านไอพี เพราะถ้าระบบมี Jitter มากก็จะทำให้การส่งข้อมูลมีความผันผวนมาก ทำให้คุณภาพของเสียงแย่ลงนั่นเอง โดยการแก้ปัญหาของ Jitter นั้นทำได้โดยการใช้บัฟเฟอร์ ถึงแม้จะลดความผันผวนได้ แต่ก็ทำให้ค่าหน่วงเวลามากขึ้นเช่นกัน ตามปกติของการสื่อสารด้วยเสียง ค่า Jitter ควรจะน้อยกว่า 50 มิลลิวินาที (20 มิลลิวินาทีสำหรับคุณภาพเทียบเท่ากับโทรศัพท์ปกติ)

2.7.5 แพ็กเก็ตที่สูญหาย (Packet Loss)

แพ็กเก็ตที่สูญหายประกอบด้วยจำนวนบิตที่ผิดพลาดและแพ็กเก็ตที่ถูกดร็อปไป โดยที่จำนวนแพ็กเก็ตที่สูญหายจะมีความสำคัญมากต่อการสื่อสารข้อมูลของแอพพลิเคชัน เช่น ข้อมูลที่ใช้ในระบบหรือโปรแกรมคำนวณทางด้านการเงิน แต่อาจจะมีผลไม่มากนักสำหรับการสื่อสารด้วยเสียง เพราะอาจแค่มีเสียงรบกวนหรือขาดหายไปบ้างเล็กน้อยเท่านั้น อย่างไรก็ตาม ถ้ามีจำนวนแพ็กเก็ตที่สูญหายมีมากเกินไป ก็จะทำให้คุณภาพของการสนทนาลดลงด้วย ตามปกติแล้ว อัตราการสูญหายของแพ็กเก็ตในระบบโทรศัพท์ผ่านไอพีไม่ควรมากกว่า 5 เปอร์เซ็นต์ หรือ 1 เปอร์เซ็นต์สำหรับคุณภาพเสียงที่สื่อสารด้วยโทรศัพท์ปกติ

2.8 วิธีการวัดค่าคุณภาพของเสียง

ในการพัฒนาต่อยอดซอฟแวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพีเรื่องของความมั่นคงไม่ใช่ประเด็นสำคัญเพียงอย่างเดียว แต่คุณภาพเสียงหรือคุณภาพการให้บริการหลังจากมีการพัฒนาด้านความมั่นคงก็เป็นประเด็นสำคัญเช่นกัน ดังนั้นจึงจำเป็นต้องมีการวัดคุณภาพเสียงเพื่อดูผลว่าคุณภาพเสียงของระบบ VoIP หลังจากพัฒนาด้านความมั่นคง ดีขึ้นหรือลดลงอย่างไร โดยที่วิทยานิพนธ์นี้ได้เลือกใช้วิธีการเพื่อใช้ในการวัดคุณภาพเสียงหรือคุณภาพการให้บริการดังนี้

2.8.1 Mean Opinion Score (MOS)

Mean Opinion Score (MOS) [23, 24] เป็นวิธีการวัดคุณภาพเสียงวิธีแรกที่ได้รับการยอมรับและเป็นมาตรฐาน MOS เป็นค่าที่ใช้วัดคุณภาพเสียงจากเครือข่ายโทรศัพท์ ซึ่งได้มีการกำหนดเป็นมาตรฐานโดย ITU P.800 เป็นการวัดคุณภาพโดยใช้ความคิดเห็นหรือความพึงพอใจของผู้ใช้งาน โดยต้องใช้คนมาทดสอบความพึงพอใจจำนวนมาก ซึ่งก็แน่นอนว่าต้องเอาคนที่มีทักษะในการฟัง การแยกแยะพอสมควร และความเชื่อถือได้หรือไม่นั้น ก็ขึ้นกับจำนวนคนที่นำมาทดสอบนั้นยิ่งมากเท่าไร ก็ยิ่งเชื่อถือได้มากขึ้นเท่านั้น โดยให้ฟังไฟล์ออดิโอต่างๆ ในสภาพที่เงียบที่สุด และให้ผู้ฟังแต่ละคนให้คะแนนซึ่งมีตั้งแต่ 1-5 คะแนน โดยที่ คะแนน 1 คุณภาพเสียงแย่ทำให้ผู้ใช้ไม่พอใจในการใช้บริการ คะแนน 2 คือคุณภาพเสียงไม่ดีฟังเสียงได้ไม่ชัดเจน คะแนน 3 คุณภาพเสียงพอใช้อาจเสียงไม่ชัดเจนมากนักอาจจะทำให้ผู้ใช้รู้สึกหงุดหงิด คะแนน 4 คือคุณภาพเสียงดีฟังเสียงได้ชัดเจน และ คะแนน 5 คือคุณภาพเสียงยอดเยี่ยมฟังเสียงชัดเจน ดังที่แสดงในตารางที่ 2.3

ตารางที่ 2.3 ค่า MOS และระดับคุณภาพของเสียง

MOS	คุณภาพ	ลักษณะเสียง
5	ยอดเยี่ยม (Excellent)	ดีจนคาดไม่ถึง (Imperceptible)
4	ดี (Good)	ใช้ได้ดี (Perceptible)
3	พอใช้ (Fair)	น่าหงุดหงิดเล็กน้อย (Slightly Annoying)
2	ไม่ดี (Poor)	ไม่น่าพอใจ (Annoying)
1	แย่ (Bad)	ไม่พอใจ (Very Annoying)

ที่มา : [24]

การวัดค่า MOS หลังจากที่ได้คะแนนของแต่ละคนมา ก็จะทำการคำนวณหาค่าเฉลี่ยของคะแนนที่ในแต่ละ CODEC เช่น G.711 ได้คะแนนเฉลี่ย 4.3 ซึ่งถือว่าเป็นคะแนนที่ดีมาก CODEC อื่นๆ ก็จะได้คะแนนแตกต่างกันไปตามคุณภาพเสียงที่ประเมินออกมา การประเมินคุณภาพเสียงเช่นนี้เป็น Subjective คือความพึงพอใจจะขึ้นกับตัวบุคคลมีความแตกต่างกันมาก ดังนั้นจึงทำให้ต้องมีการใช้จำนวนคนมากๆ เพื่อเพิ่มความน่าเชื่อถือและลดประเด็นที่เป็น Subjective นี้ลงไป

ตารางที่ 2.4 ตัวอย่างของ CODEC และค่า MOS

ชนิดของ CODEC	Data Rate	MOS
G.711 (ISDN)	64 kbps	4.3
G.729	8 kbps	3.92
G.726 ADPCM	32 kbps	3.8
GSM FR	12.2 kbps	3.5

ที่มา : [24]

ตารางที่ 2.4 ตัวอย่างของ CODEC และค่า MOS ที่ได้และเพื่อเป็นการเพิ่มความน่าเชื่อถือในการวัดคุณภาพเสียงด้วยวิธีนี้ ทาง ITU-T ก็ได้กำหนดวิธีการทดสอบเพิ่มเติม โดยมีการกำหนดข้อความที่ใช้ทดสอบนั้น ซึ่งเป็นข้อความที่เรียกว่า Harvard Sentences ที่ในการออกเสียงจะช่วงความถี่เสียงทั้งหมดที่พบในคำพูดคำสนทนาทั่วไป ทำการบันทึกด้วยความละเอียดสูงแบบ 16 บิต ตัวอย่างของข้อความดังกล่าว ได้แก่

You will have to be very quiet.
There was nothing to be seen.
They worshipped wooden idols.
I want a minute with the inspector.
Did he need any money?

เนื่องจากวิธีการดังกล่าวนั้น จะเน้นที่คุณภาพเสียงที่ได้รับฟัง จึงมักใช้ในการทดสอบ CODEC กันมาก เป็นวิธีที่ได้รับการยอมรับกันมากที่สุด และใช้เป็นมาตรฐานในการเปรียบเทียบวิธีการอื่นๆ ว่าเชื่อถือได้มากน้อยเพียงใด โดยที่ค่า MOS ที่ยอมรับได้และเป็นไปตามมาตรฐานคือมากว่าหรือเท่ากับ 3.6 แต่วิธีการนี้จะค่อนข้างยุ่งยาก สิ้นเปลืองทั้งการหาผู้ที่มีทักษะมาจำนวนมากๆ เวลาที่ใช้ทดสอบเป็นต้น จึงทำให้มีการคิดค้นวิธีการอื่นๆ ที่จะช่วยให้การวัดคุณภาพเสียงนั้นง่ายขึ้น

2.8.2 E-Model

E-Model [12, 25, 26] เป็นรูปแบบการวัดคุณภาพเสียงที่ถูกกำหนดเป็นมาตรฐานโดย International Telecommunication Union (ITU) G.107 เป็นแบบจำลองใช้วิเคราะห์คุณภาพเสียงสำหรับวางแผนเครือข่าย โดยมีผลลัพธ์จาก E Model เป็นค่า R Factor (0-100) สามารถคำนวณกลับมาเป็นค่า MOS ซึ่งคำนวณค่า R Factor ได้จากสมการดังนี้

$$R = R_0 - I_s - I_d - I_{ef\text{-}eff} + A \quad (1)$$

โดยที่

R_0 คือ อัตราส่วนระหว่างสัญญาณต่อเสียงรบกวน (Signal to Noise Ratio)

I_s คือ ค่าบกพร่องทั้งหมดที่เกิดขึ้นมากหรือน้อยที่เกิดขึ้นพร้อมกันกับสัญญาณเสียง

I_d คือ ค่าความบกพร่องที่เกิดจากความล่าช้า (Delay)

$I_{ef\text{-}eff}$ คือ ค่าการสูญเสียของแพ็กเก็ต (Packet Loss) ที่มีผลจากความบกพร่องของอุปกรณ์

A คือ ค่าปัจจัยได้เปรียบในการเข้าถึงอุปกรณ์

เนื่องจาก R Factor เป็นการคำนวณค่าพารามิเตอร์ซึ่งเป็นสูตรที่คณิตศาสตร์ที่ซับซ้อน ได้มองว่าการคำนวณที่มีคุณภาพจะถูกกำหนดโดย ค่าความบกพร่องที่เกิดจากความล่าช้า (Delay) และค่าการสูญเสียของแพ็กเก็ต (Packet Loss) ที่มีผลจากความบกพร่องของอุปกรณ์ ซึ่งครอบคลุมการสูญเสียข้อมูลเนื่องจากการเข้ารหัสและการสูญเสียแพ็กเก็ต (Packet Loss) จึงมีการลดทอนสูตรให้ง่ายต่อการคำนวณค่า R ที่มีคุณภาพดังนี้

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

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

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

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

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

Ppl = Packet lost Probability

Ie = Equipment Impairment

Factor ค่าตามตารางที่ 2.5

Bpl = Packet Lost Robustness Factor ค่าตามตารางที่ 2.5

ตารางที่ 2.5 ค่า *Ie* และ *Bpl* ของแต่ละ CODEC

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

ที่มา : [25]

ตารางที่ 2.5 แสดงถึงค่า I_e และ *Bpl* ของแต่ละ Codec โดยวิทยานิพนธ์นี้ได้ศึกษาวิจัย Default Codec ของ FreeSWITCH นั่นคือ G.711 ดังนั้นจึงใช้ ค่า I_e = 0 และ Bpl = 4.3 ในการคำนวณ

โดยที่ทาง ITU ได้กำหนดการเปรียบเทียบค่า MOS กับค่า R Factor สอดคล้องตามสมาการ โดยที่คำนวณค่า MOS ได้ดังนี้

ค่า MOS เท่ากับ

$$MOS = \begin{cases} 1 & \text{เมื่อ } R < 0 \\ 1+0.035\ R+R(R-60)\ (100-R)7x10^{-6} & \text{เมื่อ } 0 < R < 100 \\ 4.5 & \text{เมื่อ } R > 100 \end{cases} \quad (3)$$

เมื่อนำค่า R Factor มาเปรียบเทียบกับ E-Model ตามข้อกำหนดจะได้ผลดังรูปที่ 2.5

รูปที่ 2.5 ค่า R Factor E-Model เปรียบเทียบค่ากับ MOS

โดยสามารถแบ่งระดับค่า MOS ตามมาตรฐานตามลักษณะความพึงพอใจได้ดังนี้ ระดับ Very Satisfied มากกว่า 4.3 ระดับ Satisfied 4.0 ถึง 4.29 ระดับ Some Users Dissatisfied 3.6 ถึง 3.9 ระดับ Many Users Dissatisfied 3.1 ถึง 3.6 ระดับ Nearly All Users Dissatisfied 2.6 ถึง 3.0 ระดับ Not Recommended 1 ถึง 2.5 ซึ่งจากมาตรฐานจะมีค่า R Factor ขั้นต่ำที่ยอมรับได้คือต้องมากกว่าหรือเท่ากับ 70 หรือค่า MOS มากกว่าหรือเท่ากับ 3.6 ดังนั้นระบบ VoIP ที่มีค่า MOS มากกว่า 3.6 หรือค่า R Factor มากกว่า 70 ก็แสดงว่าเป็นระบบ VoIP ที่มีคุณภาพการให้บริการในระดับที่ดี เป็นไปตามมาตรฐานที่สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (กสทช.) [27] เป็นผู้กำหนดโดยได้อ้างอิงจากมาตรฐานของ ITU-T G.107

2.9 งานวิจัยที่เกี่ยวข้อง

2.9.1 ชุดซอฟต์แวร์สำหรับโทรศัพท์ผ่านเครือข่ายไอพี

ISAN Box.A [7] ถูกพัฒนาขึ้นโดย คธาวุธ จันบัวลา และ สมนึก พ่วงพรพิทักษ์ ได้พัฒนาต่อยอดชุดซอฟต์แวร์ VoIP Open-source Software โดยได้พัฒนาขึ้นมาจากซอฟต์แวร์ Asterisk เป็นฐานในการพัฒนา ซึ่งพัฒนาให้ป้องกันการโจมตีการดักฟังการสนทนา ป้องกัน SIP Flooding ป้องกัน SIP Register Hijacking และ ป้องกัน SVMAP เพื่อสแกนหา SIP Server ที่เปิดให้บริการ เป็นต้น ซึ่งผลการพัฒนาทำให้ได้ระบบ VoIP มั่นคงปลอดภัยมากขึ้น แต่ก็ยังไม่มีการประเมินคุณภาพการให้บริการหลังจากที่เสริมความมั่นคงให้ระบบแล้ว ซึ่งงานวิจัยนี้ได้เสนอรูปแบบการแก้ไขปัญหา SIP Flooding โดยใช้ Shell Script ตั้งเวลาให้ทำงานอ่านและวิเคราะห์ไฟล์ Log เพื่อตรวจหาการโจมตีโดยอัตโนมัติ ซึ่งวิธีแก้ปัญหานี้ยังคงมีความไม่สมบูรณ์เนื่องจากว่า ในช่วงเวลาที่ Shell Script ไม่ทำงาน อาจจะมีการโจมมีเข้ามาและไม่ถูกตรวจจับอย่างทันเหตุการณ์ ซึ่งก็จะส่งผลกระทบต่อระบบ VoIP ให้เกิดการปฏิเสธให้บริการได้

EZY-PBX [8] ถูกพัฒนาขึ้นจากความร่วมมือระหว่าง สถาบันวิจัยและพัฒนาอุตสาหกรรมโทรคมนาคม (TRIDI) และ คณะเทคโนโลยีสารสนเทศมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี ซึ่งเป็นระบบซอฟต์แวร์ สำหรับการใช้งาน ระบบ Voice Over IP (VOIP) ที่เป็นภาษาไทย ซึ่งใช้งานและติดตั้งได้แบบกึ่งอัตโนมัติ เพื่อเป็นการส่งเสริมการใช้งาน ระบบ VOIP ในประเทศไทยโดยซอฟต์แวร์ดังกล่าวจะมีคุณสมบัติคือ เป็นระบบที่พัฒนาบนพื้นฐานของซอฟต์แวร์แบบ Open-source เป็นระบบที่ใช้ภาษาไทยในการปฏิสัมพันธ์กับผู้ใช้เป็นหลัก เป็นระบบที่ใช้รูปภาพ และไอคอนในการปฏิสัมพันธ์กับผู้ใช้เป็นหลัก เป็นระบบที่ถูกพัฒนาด้วยเทคโนโลยี Web service ซึ่งสามารถประยุกต์ใช้งานได้หลากหลาย เป็นระบบที่ติดตั้งง่าย โดยการติดตั้งจะรวมระบบปฏิบัติการลีนุกซ์ซอฟต์แวร์ Asterisk และระบบการปฏิสัมพันธ์แบบรูปภาพในการจัดการโครงแบบของระบบไว้ด้วยกันเป็นแบบ กึ่งอัตโนมัติ แต่ก็ยังขาดคุณสมบัติทางด้านความมั่นคงของระบบ อีกทั้งยังไม่มีการประเมินประสิทธิภาพด้านคุณภาพการให้บริการ

Asterisk Now for Thai [9] เป็นโครงการความร่วมมือระหว่าง กทช. และ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี ในการพัฒนาซอฟต์แวร์ Asterisk ให้มีความสามารถในการรองรับการใช้งานที่เป็นภาษาไทย เพื่อคนไทยโดยเฉพาะ ทั้งนี้เพื่อเป็นการสนับสนุนให้คนไทยได้ใช้งานผลิตภัณฑ์ที่เป็น Open-source และมีคุณสมบัติที่ดีเทียบเคียงกับผลิตภัณฑ์ที่มีจำหน่ายในเชิงพาณิชย์ทั่วไป อีกทั้งเพื่อเป็นการส่งเสริมการใช้งานโทรศัพท์ผ่านเครือข่าย IP ในประเทศไทยให้แพร่หลายมากขึ้น ANT ถูกพัฒนาขึ้นมาจาก Asterisk รุ่น 1.02 โดยมี การปรับปรุงส่วนเชื่อมต่อกับผู้ใช้เป็นภาษาไทย เพื่อช่วยสื่อความหมายให้กับผู้ใช้ได้เข้าใจมากยิ่งขึ้น อีกทั้งยังเพิ่มความสะดวก และความง่ายในการใช้งาน แต่ก็ยังขาดคุณสมบัติทางด้านความมั่นคงของระบบ อีกทั้งยังไม่มีการประเมินประสิทธิภาพด้านคุณภาพการให้บริการ

ISAN Secure Box [28] ถูกพัฒนาขึ้นจากซอต์ฟแวร์ FreeSWITCH โดย ประดิษฐ์ วงศ์สกุล, ปิยะณัฐ สุยังกุล และสมนึก พ่วงพรพิทักษ์ ได้พัฒนาต่อยอดชุดซอฟต์แวร์ VoIP Open-source ซึ่งมุ่งเน้นพัฒนาด้านความมั่นคง ให้ป้องกันการโจมตีการดักฟังการสนทนา ป้องกันการโจมตีแบบ SIP Flooding อีกทั้งได้พัฒนาส่วนติดต่อผู้ใช้งาน รองรับภาษาไทย สะดวกต่อการตั้งค่าใช้งาน

มีส่วนการติดตั้งที่ใช้งานง่ายแต่ก็ยังไม่มีการเสริมความมั่นคงในระบบสัญญาณ และขาดการประเมินประสิทธิภาพการให้บริการ

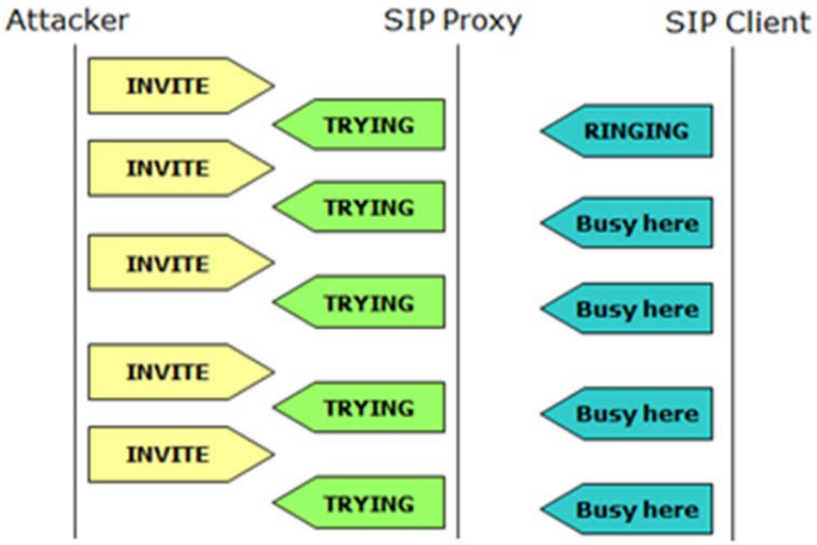
Blue Box Project [29] คือโครงการพัฒนาระบบ VoIP ที่มีการพัฒนามาจากซอฟต์แวร์ FreeSWITCH โดยที่ Blue Box ซึ่งโครงการนี้ได้เริ่มพัฒนามาตั้งแต่ปี พ.ศ. 2556 โดยเป็นช่วงเวลาพร้อมๆกันกับวิทยานิพนธ์นี้ แต่ BlueBox จะมุ่งพัฒนาระบบให้มีความสะดวก ง่ายต่อการใช้งาน โดยมีการพัฒนา Web User Interface ที่สวยงามในการใช้งาน มีการพัฒนาส่วนการติดตั้งที่สะดวก และมีการพัฒนามาจนถึงปัจจุบัน (มิถุนายน พ.ศ. 2558) BlueBox ถึงรุ่นที่ 1.0.3 แต่งอย่างไรก็ตาม โครงการ Blue Box นี้ก็ยังไม่ได้พัฒนาประสิทธิภาพด้านความมั่นคง และยังไม่มีการทดสอบประสิทธิภาพด้านคุณภาพการให้บริการ

2.9.2 ปัญหาด้านความมั่นคงของชุดซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพี

ปิยวัจน์ ค้าสบาย และ สมนึก พ่วงพรพิทักษ์ [4] ได้ทำการประเมินซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพีที่เป็นที่นิยมคือ Asterisk FreeSWITCH และ OpenSER โดยได้ออกแบบการทดลองโจมตีด้วยเทคนิควิธีต่างๆ ในเครือข่ายจำลอง ซึ่งงานวิจัยนี้ได้เลือกทดลองการโจมตีที่จะส่งผลกระทบร้ายแรงกับระบบ VoIP อันได้แก่ SIP Flooding Attack เพื่อทำให้ระบบ VoIP ปฏิเสธการให้บริการ Cancle/By Attack เพื่อยกเลิกการสนทนา และ Man in the Middle Attack (MiTM) เพื่อดักฟังเสียงสนทนา ผลจากการทดลองปรากฏว่า ชุดซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพีทั้ง 3 ชุดซอฟต์แวร์ ยังมีปัญหาและมีความเสี่ยงด้านความมั่นคงอยู่มาก คือ ยังถูกโจมตีตามรูปแบบวิธีที่เสนอในงานวิจัยนี้ได้ ซึ่งบางปัญหาที่พบเป็นปัญหาที่ร้ายแรง เช่น การดักฟังเสียงการสนทนา เพราะถ้าหากถูกดักฟังข้อมูลลับขององค์กร ความลับทางการค้า ก็อาจจะเกิดความเสียหายต่อธุรกิจได้

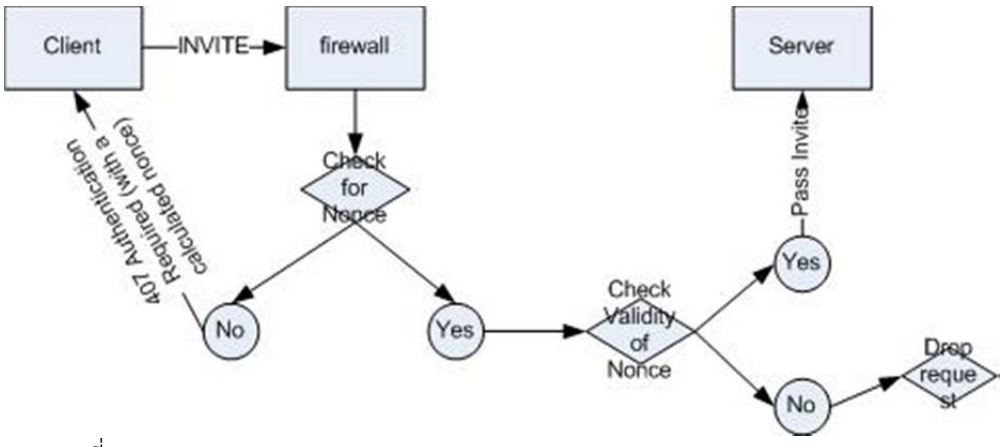
2.9.3 การโจมตี SIP Proxy ด้วยเทคนิควิธี SIP Flooding

โดยปกติในการติดต่อสื่อสารบนระบบ VoIP จำเป็นต้องมีการการสร้าง Session เพื่อใช้ในการกำหนดข้อตกลงหรือรายละเอียดของการสื่อสาร ซึ่งใช้โพรโทคอล Session Initiation Protocol (SIP) ในการสร้างเซสชั่น ด้วยมาตรฐานของ SIP แล้ว จะต้องมีการส่งข้อความ SIP ทั้ง ข้อความร้องขอและข้อความตอบสนองโต้ตอบกันระหว่าง SIP Proxy กับ ผู้ที่ต้องการสื่อสารด้วย จึงทำให้เกิดเป็นช่องโหว่ให้มีการโจมตีจากผู้ไม่หวังดี ด้วยการส่งข้อความ Invite มายัง SIP Proxy อย่างต่อเนื่อง จำนวนมากและอัตราเร็วกว่าปกติ ทำให้ SIP Proxy ส่งข้อความตอบสนองข้อความ Invite ดังกล่าว จนไม่สามารถให้บริการผู้ใช้ทั่วไปได้ และส่งผลให้ CPU มีภาระงานหนักมากขึ้น จึงทำให้ระบบ VoIP ล้มเหลวลงในที่สุดดังแสดงการโจมตีในรูปที่ 2.6 มีนักวิจัยคือ Mark D. Collier [5] ได้พัฒนา Script ที่ใช้ในการโจมตี SIP Flooding ไว้ในระบบปฏิบัติการ Backtrack ในหมวดของ VoIP Penetration Test ซึ่งภายหลังได้เปลี่ยนมาเป็นระบบปฏิบัติ Kali Linux



รูปที่ 2.6 การโจมตี SIP Flooding

มีงานวิจัยที่กล่าวถึงปัญหาการโจมตีด้วยเทคนิค SIP Flooding เช่น งานวิจัยของ Deng X และ Lee C [6] ที่ได้นำเสนอถึงปัญหาและผลกระทบที่เกิดขึ้นกับ SIP Proxy เมื่อมีการโจมตี SIP Flooding และได้เสนอแนวคิดการป้องกัน SIP Flooding ด้วยวิธีการตรวจสอบค่าเฉพาะของ Session หรือที่เรียกว่าค่า Nonce ซึ่งจะนำมาคำนวณร่วมกับ CallID และ Source IP และใช้ขบวนการเข้ารหัสร่วมด้วย โดยให้ Firewall ทำหน้าที่ตรวจสอบและกลั่นกรองเพ็กเก็ตที่อาจเป็นการโจมตี โดยถ้าหากตรวจสอบค่า Nonce แล้วพบว่ามีลักษณะเป็นการโจมตี Firewall ก็จะไม่ปล่อยให้แพ็กเก็ตนั้นไปถึง SIP Proxy ดังตัวอย่างในรูปที่ 2.7



ที่มา : [6]

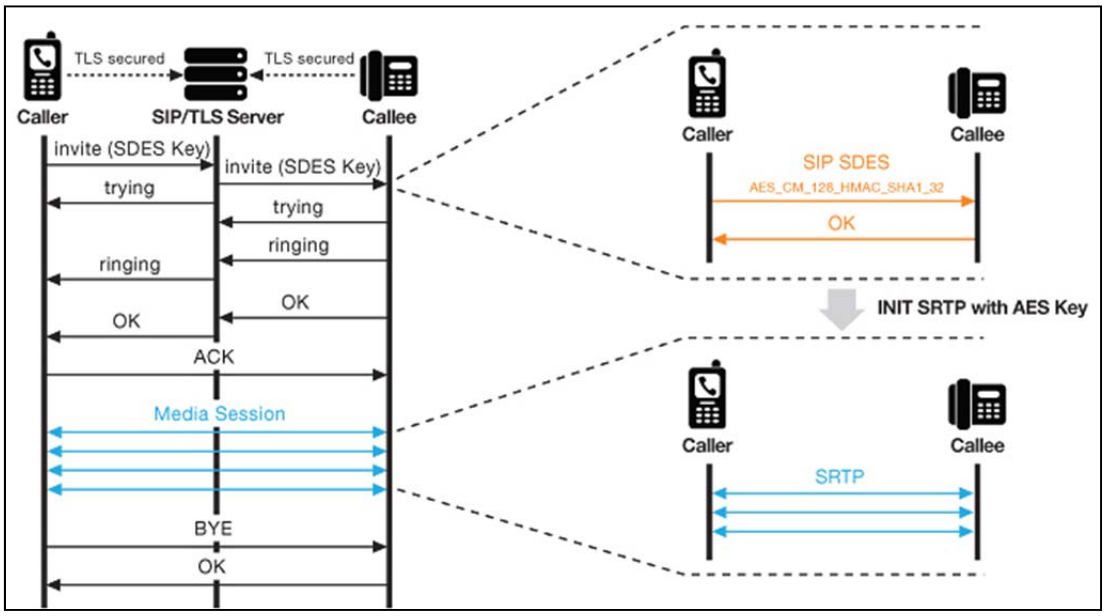
รูปที่ 2.7 การตรวจสอบค่า Nonce ของ Firewall

จากการวิเคราะห์งานวิจัยนี้จะพบว่า หน้าที่หลักในการตรวจจับการโจมตีจะอยู่ที่อุปกรณ์ Firewall ซึ่งในกระบวนเข้ารหัส CallID และ Source IP ก็จะส่งผลให้เกิดภาระงานของระบบที่เพิ่มขึ้น และเกิด Overhead ของเครือข่ายขึ้นได้ อีกทั้งงานวิจัยนี้ไม่มีระบบการรายงานและการแจ้งเตือนการโจมตีที่เข้าถึงผู้ดูแลระบบได้อย่างรวดเร็วและทั่วถึง อย่างไรก็ตามงานวิจัยนี้ก็ยังไม่ได้มีการทดลองนำแนวคิดการแก้ไขปัญหานี้ไปประยุกต์ใช้และยังไม่มีการทดสอบประสิทธิภาพในการป้องกันปัญหา SIP Flooding

ซึ่งต่างจากงานในวิทยานิพนธ์นี้ที่ได้เสนอวิธีการตรวจจับการโจมตีให้โพรโทคอล SIP มีคุณสมบัติสามารถตรวจจับการโจมตีได้ด้วยตัวเอง ตอบสนองได้ทันต่อเหตุการณ์ และมีระบบการรายงานและการแจ้งเตือนการโจมตีผ่านทางเฟซบุ๊กอีกด้วย

2.9.4 Security Real-time Transport Protocol (SRTP)

SRTP [30, 31] คือรูปแบบการส่งข้อมูล Multimedia ซึ่งจะทำการทำงานโดยการเข้ารหัสข้อมูล รับรองความถูกต้องและช่วยในเรื่องขอความมั่นคงปลอดภัยโดยนำมาใช้ใน VoIP โดยเฉพาะการส่งข้อมูลในระดับบิตและการแปลงสัญญาณเสียง เช่น G.729, iLBC, MELP เพราะมันสามารถใช้กับการบีบอัดส่วนหัวและไม่มีผลกระทบต่อคุณภาพการให้บริการ นอกจากนี้ยังสามารถใช้กับ JPEG, MPEG2, MPEG4 และวิดีโอสตรีมได้อย่างปลอดภัย ในโปรแกรมมัลติมีเดีย SRTP จะใช้งานได้อย่างมีประสิทธิภาพทั้งในเครือข่ายแบบมีสายและไร้สาย SRTP เป็นโพรโทคอลทางด้านความปลอดภัยในการส่งข้อมูลที่ทำงานอยู่ระหว่าง Application Layer และ Transport Layer โดยมีการสร้าง SRTP แพ็คเก็ต แล้วส่งต่อแพ็คเก็ตนี้ไป ถึงผู้รับในทำนองเดียวกันก็แปลง SRTP แพ็คเก็ตที่รับเข้า ซึ่งการเข้ารหัสข้อมูล SRTP มีการเข้ารหัสและใช้หลักการ Session Key มีวิธีการแลกเปลี่ยนกันอย่างปลอดภัยดังแสดงในรูปที่ 2.8



ที่มา: [30]

รูปที่ 2.8 การทำงาน Security Real Time Transport Protocol

การประเมินคุณภาพการให้บริการของ Voice over Internet Protocol

1) คุณภาพเสียงของ VoIP แบบปลอดภัย

Radman [13] ได้วิจัยการใช้งานโทรศัพท์แบบปลอดภัยซึ่งได้ผลการวิจัยคือ Voice over Internet Protocol (VoIP) มีปัญหาที่สืบเนื่องมาจากการแก้ไขปัญหาทางด้านความมั่นคงปลอดภัยของระบบ VoIP คือ ปัญหาคุณภาพการในให้บริการ Quality of Service (QoS) เพราะเมื่อมีการแก้ไขปัญหาเรื่องความปลอดภัยโดยวิธีต่างๆ ก็จะส่งผลต่อ QoS ของระบบ ซึ่งค่า Packet Loss, Delay, Jitter และอัลกอริทึมในการเข้ารหัสก็จะส่งผลที่โดยตรงกับคุณภาพการให้บริการของระบบ แต่พบว่ามีการเลือกใช้อัลกอริทึมที่มาศึกษาเปรียบเทียบไม่สมเหตุสมผล เช่นบางอัลกอริทึมที่เลือกมาไม่เป็นที่นิยม

2) คุณภาพเสียงของมาตรฐาน CODEC G.711, G.723 และ G.729

ศุภชัย คลังทอง พรพิมล ฉายรัสมี และ สุขสันต์ พาณิชพาพิบูล [15] ได้ทำการวิจัยเกี่ยวกับการ Evaluating Voice กรณีศึกษาการเชื่อมต่อระหว่างโครงข่ายโทรศัพท์ผ่านไอพีด้วยเลขหมายในหมวด 06 กับโครงข่ายโทรศัพท์พื้นฐานและโครงข่ายโทรศัพท์เคลื่อนที่ในประเทศไทย ซึ่งได้ผลคือ การเชื่อมต่อสื่อสารในรูปแบบโทรศัพท์ผ่านไอพีในหมวดเลขหมาย 06 ไปยังโครงข่ายโทรศัพท์แบบอื่นๆ ในประเทศไทย ยังไม่มีการให้บริการอย่างเป็นรูปธรรม เนื่องจากข้อจำกัดทางด้านเทคนิคของผู้ให้บริการโทรศัพท์ รวมไปถึงความต้องการทางด้านคุณภาพเสียงของกลุ่มผู้บริโภคซึ่งการสื่อสารในรูปแบบโทรศัพท์ผ่านไอพีไม่สามารถตอบสนองความพึงพอใจได้ งานวิจัยนี้ศึกษาคุณภาพของการสื่อสารและการเชื่อมต่อโดยใช้ E-Model ตามมาตรฐาน ITU-T G.107 ซึ่งทดสอบที่มาตรฐาน CODEC G.711, G.723 และ G.729 ภายใต้สมมติฐานการส่งผ่านขนาด Voice Payload ของแต่ละมาตรฐาน CODEC ไปบนโพรโทคอล ICMP รวมไปถึงการวัดค่าพารามิเตอร์มาตรฐานและคุณภาพการให้บริการโทรคมนาคมประเภทเสียงตามประกาศคณะกรรมการกิจการโทรคมนาคมแห่งชาติ (กทช.) ผลการทดสอบตามมาตรฐาน CODEC ดังกล่าวปรากฏว่าค่า MOS และค่า R-value รวมไปถึงคุณภาพการให้บริการโทรคมนาคมประเภทเสียงอยู่ในระดับที่สูงกว่ามาตรฐานที่ กทช. กำหนด แต่ทั้งนี้ต้องขึ้นอยู่กับตัวแปรต่างๆ ไม่ว่าจะเป็นความแปรปรวนของเวลาหรือการประวิงเวลาที่ใช้ในการเดินทางของแพ็กเก็ตที่เป็นสัญญาณเสียง ซึ่งจะทำให้ค่าพารามิเตอร์มาตรฐานทางด้านคุณภาพเสียงมีการเปลี่ยนแปลง ดังนั้นปัจจัยต่างๆ เหล่านี้จึงเป็นประเด็นที่ต้องให้ความสำคัญ

3) คุณภาพเสียงของการใช้ IPSec ในการเข้ารหัสเสียง

Alexandre [32] ได้ทำการวิจัย Evaluating Voice Speech Quality in 802.11b Networks with VPN/IPSec เพื่อวัดคุณภาพเสียงที่ของเครือข่ายที่ใช้ IPsec มาแก้ไขปัญหาเรื่องความมั่นคงปลอดภัยของข้อมูลเสียง ซึ่งจะทำการเข้ารหัสเนื้อแพ็กเก็ตทำให้ไม่สามารถดักอ่านข้อมูลนั้นๆ ได้ แต่ก็พบปัญหาเรื่อง Over head ในการเข้ารหัสตาม ซึ่งมีผลกระทบต่อคุณภาพของเสียง ดังนั้นงานวิจัยจึงได้ทำการวัดเปรียบเทียบค่าคุณภาพการให้บริการ Mean Opinion Score (MOS)

โดยใช้วิธีการเปรียบเทียบการวัดค่าจาก E-Model ซึ่งใช้หลักการคำนวณทางคณิตศาสตร์ที่นำเอาค่า Packet loss และ Delay เข้ามาคำนวณ โดยได้เปรียบเทียบอัลกอริทึมเข้ารหัสที่ต่างกันคือ ไม่เข้ารหัส AES และ 3DES ผลปรากฏว่าค่า MOS ของการไม่เข้ารหัสจะมีค่าสูงที่สุด รองมาคือ AES และ 3DES

ตามลำดับ จะเห็นได้ว่าการเข้ารหัสข้อมูลเสียงด้วยอัลกอริทึมแบบต่างๆ จะส่งผลต่อคุณภาพเสียงที่แตกต่างกัน ดังนั้น จึงควรพิจารณาเลือกใช้วิธีเข้ารหัสที่เหมาะสมและปลอดภัย

2.9.5 การวัดเวลาในการทำกิจกรรมต่างๆบนส่วนติดต่อผู้ใช้งานโดยใช้ KLM

Keystroke-Level Model (KLM) ถูกพัฒนาขึ้นในปี ค.ศ. 1983 โดย Card [33] และคณะ ซึ่งเป็นโมเดลที่ใช้วัดเวลาที่ใช้ในการกระทำกิจกรรมบางอย่างบนส่วนติดต่อผู้ใช้งานโดยเป็นส่วนหนึ่งของ Goal Operator Method Selection (GOMS) rules ใน Cognitive Modeling ซึ่งการคำนวณเวลาในการทำกิจกรรมต่างๆ จะมีสูตรในการคำนวณดังนี้

$$T_{time} = T_{acquire} + T_{execute} \quad (4)$$

เมื่อ

T_{time} คือ เวลาทั้งหมดในการทำกิจกรรม

$T_{acquire}$ คือ เวลาในการได้มาของงาน

$T_{execute}$ คือ การปฏิบัติงานที่ได้มา

โดยที่การคำนวณเวลาจากการทำกิจกรรมบนส่วนติดต่อผู้ใช้งานนั้นจะมีการกำหนดการกระทำและเวลาที่ใช้อย่างเหมาะสมไว้ดังตารางที่ตารางที่ 2.6

ตารางที่ 2.6 เวลาที่ใช้ในการทำแต่ละกิจกรรมบนส่วนติดต่อผู้ใช้งาน

Operator	Description	Time(sec)
K	Pressing a single key or button	
	Average skilled typist (55 wpm)	0.20
	Average non-skilled typist (40 wpm)	0.28
	Pressing shift or control key	0.08
	Typist unfamiliar with the keyboard	1.20
P	Pointing with a mouse or other device on a display to select an object. This value is derived from Fitts' Law which is discussed below.	1.10
P1 or K	Clicking the mouse or similar device	0.20
H	Bring 'home' hands on the keyboard or other device	0.40
M	The response time is counted only if it causes the user to wait.	1.35
R(t)	The response time is counted only if it causes the user to wait.	t

ที่มา : [33]

มีงานวิจัยของ Kieras [34] ได้อธิบายถึงการใช้งาน KLM โดยจำลองการใช้ KLM ในกิจกรรมต่างๆ โดยในงานวิจัยของ Kieras ได้ทำการทดลองคำนวณเวลาในการลบไฟล์ โดยเปรียบเทียบกับแบบเดิมที่ออกแบบไว้ และการออกแบบใหม่โดยใช้วิธี KLM โดยผลกาทดลองปรากฏว่า ถ้าใช้การออกแบบแบบเดิมจะใช้เวลา 12.3 วินาที แต่เมื่อเปลี่ยนมาใช้การออกแบบแบบใหม่โดยใช้วิธี KLM เข้ามาวัดคำนวณเวลาจะใช้เวลา 5.06 วินาที

จากการศึกษางานวิจัยเกี่ยวกับ KLM วิทยานิพนธ์นี้จึงมีแนวคิดที่จะนำทฤษฎีดังกล่าวมาประยุกต์ใช้ในการวัดและคำนวณเวลาที่ใช้ในการทำกิจกรรมต่างบนส่วนติดต่อผู้ใช้งาน โดยเปรียบเทียบระหว่างการใช้งาน VoIP เดิม และระบบ ISANBox.F ที่ได้พัฒนาขึ้นมาใหม่

2.9.6 วิธีการทดสอบประสิทธิภาพทางเครือข่าย

รูปแบบการทดสอบประสิทธิภาพทางเครือข่ายหลักมีด้วยกัน 3 วิธี [35] ได้แก่ Analytical Modeling, Simulation และ Measurement โดยมีรายละเอียดดังนี้

1) Analytical Modeling

Analytical Modeling เป็นการใช้โมเดลคณิตศาสตร์เพื่อออกแบบและคำนวณ ซึ่งวิธีนี้จะแก้ปัญหาได้เพียงปัญหาที่ไม่ซับซ้อน นิยมใช้กับการแก้ปัญหาที่ไม่ใหญ่มากนัก

2) Simulations

Simulations เป็นการใช้โปรแกรมจำลองเครือข่ายเพื่อใช้ในการวิเคราะห์ปัญหาที่ซับซ้อนได้มากกว่า แบบแรกแต่ยังมีข้อเสียเรื่องคือการทดสอบแบบนี้เป็นการจำลองเครือข่าย จึงอาศัยความน่าจะเป็นดังนั้นจะทำให้ได้บริบทรวมทั้งผลรับที่อาจจะคาดเคลื่อนจากเครือข่ายจริง

3) Measurement เป็นการวัดค่าที่ได้จากการทดลองในเครือข่ายจริงแบ่งได้ 2 แบบ ดังนี้

1. Real System เป็นการวัดค่าจริงจากระบบจริง แต่ค่าที่ได้จากวิธีนี้อาจจะไม่สามารถนำมาใช้งานได้ เพราะเป็นการวัดจากระบบจริง ซึ่งไม่ถูกควบคุมค่าพารามิเตอร์ต่าง ๆ ที่มีผลต่อค่าที่วัดได้ แต่วิธีการนี้มีข้อดีคือได้เห็นถึงสภาพการใช้งานจริง ซึ่งส่วนใหญ่จะใช้เป็นขั้นตอนสุดท้ายที่ผ่านกาทดสอบในแบบอื่นมาแล้ว

2. Test-beds เป็นการสร้างเครือข่ายจำลองเพื่อทดสอบที่มีลักษณะคล้ายกับเครือข่ายจริงแต่มีขนาดเล็กกว่า สามารถควบคุมพารามิเตอร์ต่าง ๆ ได้ สามารถวัดประสิทธิภาพและประสิทธิผลได้ดีกว่า

ในวิทยานิพนธ์ได้เลือกวิธีทดสอบประสิทธิภาพด้วยวิธี Test-beds เพราะการวัดประสิทธิภาพและประสิทธิผลด้านความมั่น คงจะเห็นผลได้ดีกว่า อีกทั้งปัญหาความมั่นคงเป็นการโจมตีที่ไม่สามารถทำในเครือข่ายจริงได้ เพราะอาจจะทำให้ผู้ใช้งานจริงไม่สามารถใช้งานได้ และยังมีความผิดทางจริยธรรมกฎหมายอีกด้วย

บทที่ 3

วิธีดำเนินการวิจัย

วิทยานิพนธ์นี้ได้มีมุ่งเน้นศึกษาปัญหาและแนวทางแก้ไขปัญหาด้านความมั่นคงของระบบ Voice Over Internet Protocol ตั้งแต่ในระดับซอฟต์แวร์เสรี (VoIP Open-source Software) ไปถึงระดับ Signaling Protocol คือการเสนอวิธีการป้องกัน SIP Flooding ที่มีประสิทธิภาพ ดังแสดงในภาพรวมงานวิจัยในรูปที่ 3.1

รูปที่ 3.1 ภาพรวมงานวิจัย

จากภาพรวมงานวิจัยในรูปที่ 3.1 งานวิจัยได้พัฒนาปรับปรุงประสิทธิภาพด้านความมั่นคงของซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพี โดยวิทยานิพนธ์ได้เลือกซอฟต์แวร์ FreeSWITCH มาเป็นฐานในการพัฒนา ซึ่งการพัฒนาต่อยอดทางด้านความมั่นคงของงานวิจัยก่อนหน้า ISAN Secure Box [28] ให้มีความมั่นคงในระดับโพรโทคอลสัญญาณมากยิ่งขึ้น อีกทั้งยังได้เสนอแนวคิดการปรับปรุงวิธีแก้ไขปัญหา SIP Flooding ให้มีประสิทธิภาพมากขึ้นโดยการปรับแก้ที่โพรโทคอล SIP โดยตรง และพัฒนาต้นแบบโปรแกรมที่สนับสนุนการทำงานตามแนวคิดที่ได้ออกแบบ

3.1 เครื่องมือที่ใช้ในงานวิจัย

3.1.1 ด้านซอฟต์แวร์

1) Phonerlite

Phonerlite [36] คือซอฟต์แวร์ที่ทำหน้าที่เป็น Softphone ทำหน้าที่เป็นเหมือนเครื่องโทรศัพท์ ใช้ติดตั้งที่เครื่องคอมพิวเตอร์เพื่อใช้ในการติดต่อสื่อสารบนระบบ VoIP ซึ่งมีข้อดีคือเป็นโปรแกรมที่สนับสนุนการตั้งค่าใช้งานโพรโทคอลด้านความมั่นคงเช่น SRTP, SIPS เป็นต้นอีกทั้งยังสามารถเลือกใช้ CODEC ได้อย่างหลากหลาย มีคุณสมบัติพื้นฐานที่จำเป็นในการใช้โทรศัพท์ เช่น การรับสายอัตโนมัติ การถือสายรอ การโทรซ้ำเลขหมายล่าสุด เป็นต้น อีกทั้งยังเป็นซอฟต์แวร์ที่ตั้งค่าใช้งานง่ายและไม่มีค่าใช้จ่ายในการนำใช้งานอีกด้วย

2) Comview

Comview [37] คือ ซอฟต์แวร์ที่ใช้วิเคราะห์ระบบเครือข่ายได้ทั้งเครือข่ายแบบสายและไร้สายโดยที่ซอฟต์แวร์สามารถจับแพ็กเก็ตและอ่านค่าต่างๆ ขึ้นมาแสดงผลได้อย่างหลากหลาย สามารถวิเคราะห์ปัญหาต่างๆ ได้ในเชิงลึก โดยเฉพาะฟังก์ชันในการวิเคราะห์ข้อมูลคุณภาพการให้บริการของ VoIP ซึ่งโปรแกรมสามารถคำนวณค่า R Factor และค่า MOS จากปัจจัยทางเน็ตเวิร์ค เช่น ค่า Packet loss ค่า Delay และ jitter ตามแบบการคำนวณของ E-Model ได้อย่างสมบูรณ์และถูกต้องตามมาตรฐาน และสามารถวิเคราะห์แพ็กเก็ต วัดคุณภาพการให้บริการได้ทั้งในโพรโทคอล SIP และ H.323 Commview ทำงานได้ในระบบปฏิบัติการ Windows XP , Vista, 7, 8

3) Wireshark

Wireshark [38] คือซอฟต์แวร์ประเภท Network Monitoring ที่ใช้ในการวิเคราะห์ตรวจสอบระบบเครือข่าย สามารถทำการตรวจจับแพ็กเก็ตต่างๆ และออกรายงานได้ในรูปแบบต่างเช่น กราฟ ตาราง เป็นต้น สามารถใช้กลั่นกรองโพรโทคอลที่ต้องการวิเคราะห์ตรวจสอบได้ออย่างแม่นยำ เป็นซอฟต์แวร์ที่ตั้งค่าใช้งานง่ายและไม่มีค่าใช้จ่ายในการนำใช้งานจึงเป็นที่นิยมของใช้งานในกลุ่มผู้ดูแลระบบเครือข่าย

4) Cain and Abel

Cain and Abel [39] คือซอฟต์แวร์ที่ใช้ทดสอบช่องโหว่ด้านความมั่นคงของระบบเครือข่าย ซึ่งซอฟต์แวร์นี้ก็เป็นที่นิยมนำมาใช้งานในการทดลองหรือวิจัยทางด้านความมั่นคง เนื่องจากใช้งานง่ายไม่ซับซ้อน โดยที่ผู้ใช้งานทั่วก็สามารถใช้โปรแกรมนี้ได้โดยที่ไม่จำเป็นต้องมีความรู้ทางด้านเครือข่ายมาก อื่น อีกทั้งยังเป็นซอฟต์แวร์ที่ตั้งค่าใช้งานง่ายและไม่มีค่าใช้จ่ายในการนำใช้งานอีกด้วย

5) Kali Linux

Kali Linux [40] เป็นระบบปฏิบัติการที่รวมเอาเครื่องมือในการทดสอบความมั่นคงของระบบเครือข่ายเอาไว้ด้วยกัน โดยจะครอบคลุมการโจมตีในระดับต่างๆ ของเครือข่าย อีกทั้งยังมีความยืดหยุ่นในการเข้าไปปรับแต่ง Script หรือชุดคำสั่งต่างๆ ที่ใช้ในการโจมตี อีกทั้งยังมี Framework ต่างๆ ที่น่าสนใจในการทดสอบความมั่นคง จึงเป็นที่นิยมของนักวิจัยที่นำมาใช้ในการเป็นฐานในการพัฒนาแก้ปัญหาด้านความมั่นคง

6) Jain-SIP

Jain-SIP [41] เป็น Library ในภาษาจาวา ที่ถูกพัฒนาให้ใช้ในการจัดการ Signaling Protocol และสร้าง SIP Stack ตามที่มาตรฐาน SIP (RFC 3261) กำหนด โดยจะทำงานในลักษณะการสร้าง Session ในการติดต่อสื่อสาร ตกลงเจรจาพารามิเตอร์ต่างๆ รวมทั้งใช้ในการส่งกุญแจในการเข้ารหัสข้อมูลเสียงอีกด้วย ซึ่งใน Jain-SIP มีคลาสต่างๆ ให้เรียกใช้ โดยเฉพาะ SIP Factory สร้าง SIP Stack ที่ใช้ในการส่งข้อความ Invite และข้อความ Response ตามที่ได้กำหนดไว้ในมาตรฐานโพรโทคอล SIP

7) Facebook API

Facebook API [42] เป็น API ในภาษา PHP ซึ่งเป็นที่นิยมของกลุ่มนักพัฒนา โดยเฉพาะในกลุ่ม Web Application Developer ที่มีการพัฒนาเว็บแล้วเรียกใช้คุณสมบัติต่างๆ ที่ Facebook API กำหนดให้ใช้งาน เช่น การให้สิทธิอนุญาตในการโพสต์ข้อความบนสถานะหรือในกลุ่ม สถิติการกดชอบ สถิติการเข้าชมหน้าแฟนเพจ เป็นต้น

3.1.2 ด้านฮาร์ดแวร์

1) เครื่อง VoIP Server

เครื่อง VoIP Server: Intel(R) Core(TM) 2 Duo CPU E7300 2.66 GHz, 4 GB of RAM, 10/100 Mbps Ethernet interface card

2) เครื่อง Client

เครื่อง Client Microsoft Windows 7, Intel(R) Core(TM)2 Duo CPU 2.0 GHz, 4 GB of RAM, 10/100 Mbps Ethernet interface card

3) อุปกรณ์เครือข่าย

อุปกรณ์ Switch Cisco SF200-48 (SLM248GT-EU) 48-port , Unshielded Twisted Pair Cat 5e Cable

3.2 ปรับปรุงประสิทธิภาพด้านความมั่นคงและทดสอบคุณภาพการให้บริการของซอฟต์แวร์ FreeSWITCH

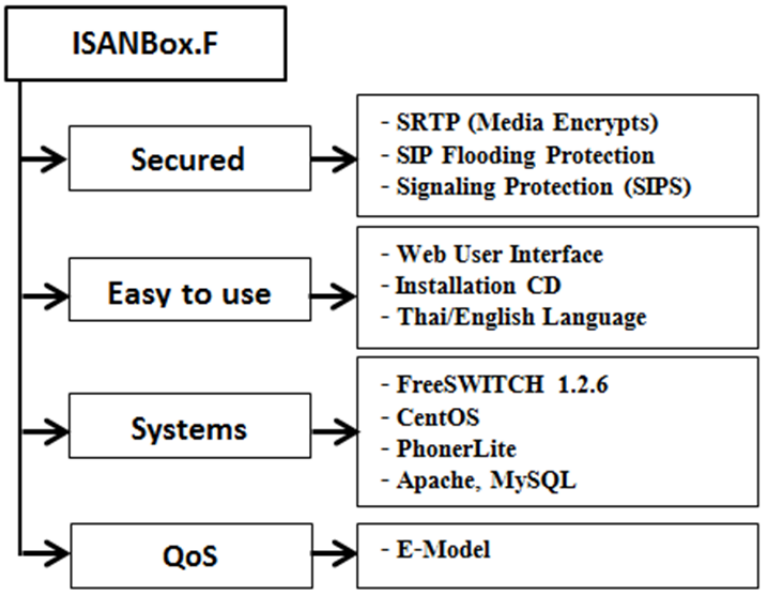
เนื่องจากคุณสมบัติทางด้านความมั่นคงและคุณภาพการให้บริการ ความนิยมของผู้ใช้งาน และคุณภาพการให้บริการตามหัวข้อ 2.5.2 วิทยานิพนธ์จึงได้เลือกใช้ซอฟต์แวร์ FreeSWITCH มาเป็นฐานในการพัฒนาให้เป็นชุดซอฟต์แวร์สำหรับโทรศัพท์ผ่านอินเทอร์เน็ต ซึ่งในช่วงเวลาที่ดำเนินการของวิทยานิพนธ์นี้ก็ได้มีกลุ่มนักพัฒนาได้พัฒนาชุดซอฟต์แวร์ BlueBox ที่ใช้ซอฟต์แวร์ FreeSWITCH มาเป็นฐานในการพัฒนาเช่นเดียวกัน แต่จะเน้นการพัฒนาในเรื่องของส่วนติดต่อผู้ใช้งานเป็นหลักและไม่ได้มีการพัฒนาประสิทธิภาพด้านความมั่นคง ต่างจากวิทยานิพนธ์นี้ที่เสนอการพัฒนาประสิทธิภาพด้านความมั่นคงของ FreeSWITCH และทำการประเมินคุณภาพการให้บริการให้ทราบคุณภาพการให้บริการหลังจากที่มีการพัฒนาด้านประสิทธิภาพด้านความมั่นคงแล้วว่าเป็นไปตามที่มาตรฐานกำหนดหรือไม่ และพัฒนาส่วนติดต่อผู้ใช้งานและส่วนการติดตั้งที่ใช้งานง่าย ซึ่งมีการออกแบบและพัฒนาระบบดังนี้

3.2.1 ออกแบบและพัฒนาระบบ

วิทยานิพนธ์นี้ได้นำซอฟต์แวร์สำหรับโทรศัพท์ผ่านเครือข่ายไอพีคือ FreeSWITCH ซึ่งเป็นซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพีที่ถูกพัฒนาขึ้นเมื่อปี ค.ศ. 2006 โดย Minessale และคณะ ซึ่งเป็นอดีตนักพัฒนาของ Asterisk มีจุดประสงค์เพื่อแก้ปัญหาเรื่องประสิทธิของ Asterisk จึงได้พัฒนา FreeSWITCH ขึ้น FreeSWITCH ทำหน้าที่เป็น IP-PBX และเนื่องด้วยการออกแบบได้ดีกว่า Asterisk ทำให้รองรับการทำงานได้มากกว่า Asterisk ประมาณ 10 เท่า [10, 11] โดยยังมีความเสถียรมากกว่า รวมไปถึงยังมีความเป็น SIP Standard มากกว่า Asteirsk เนื่องจากใช้ SIP Stack ของ Sofia [43] และมีการใช้ SQLlite ในส่วนใหญ่ของการเก็บค่าปรับแต่งและการทำงานส่วนใหญ่ของระบบ และที่น่าสนใจคือการรองรับการทำงานร่วมกับ VoIP Protocol อื่นๆ เช่น Google Talk โดยใน FreeSWITCH 1.0.6 เป็นต้นมายังมีฟังก์ชันสนับสนุนการทำงานในหลายๆ ด้าน เช่น SRTP, ZRTP

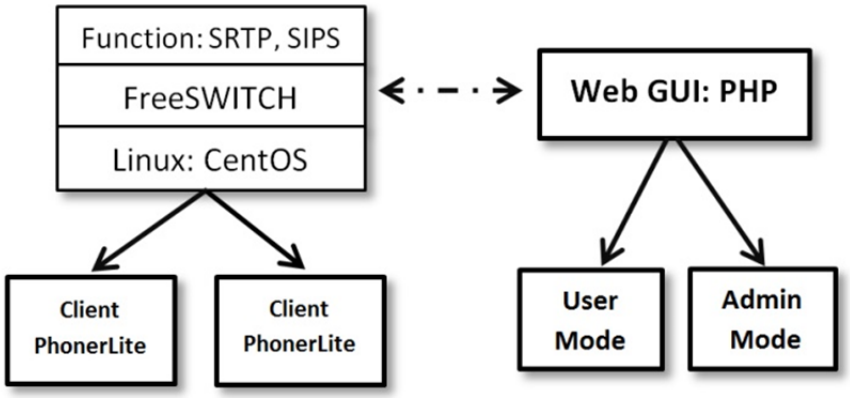
แต่อย่างไรก็ตาม FreeSWITCH ยังมีความเสี่ยงด้านความมั่นคง เนื่องจากผู้ใช้งานส่วนใหญ่จะใช้งานที่ค่าเริ่มต้นของระบบ ไม่มีการปรับแต่งด้านความมั่นคง ทั้งนี้อาจเป็นเพราะความยุ่งยาก ความไม่สะดวก ขาดทักษะการใช้งาน จึงทำให้เกิดช่องโหว่ทางด้านความมั่นคงขึ้นได้ เช่น การดักรับและปลอมแปลงแพ็กเก็ต RTP การโจมตีแบบ SIP Flooding ดังนั้นวิทยานิพนธ์นี้จึงได้เสนอการต่อยอด FreeSWITCH เพื่อเพิ่มประสิทธิภาพด้านความมั่นคง พัฒนาส่วนติดต่อผู้ใช้งานให้ใช้งานง่าย พัฒนาส่วนการติดตั้งที่ง่ายต่อการใช้งาน และได้ตั้งชื่อระบบที่ได้พัฒนาขึ้นว่า “ISANBox.F”

การพัฒนาระบบ ISANBox.F ได้ออกแบบโครงสร้างให้ใช้ Software Open-source ทำการพัฒนาอยู่บนระบบปฏิบัติการ CentOS และใช้ VoIP Software คือ FreeSWITCH 1.2.6 ซึ่งเป็นรุ่นที่คงที่ ใช้ Apache เป็น Web Server ใช้ฐานข้อมูล MySQL ใช้โปรแกรม PhonerLite ทำหน้าที่เป็น Client ในการโทรติดต่อสื่อสาร พัฒนาส่วนติดต่อผู้ใช้งานจากภาษา PHP และในด้านการประเมินคุณภาพการให้บริการด้วยวิธี E-Model ดังแสดงโครงสร้างของระบบในรูปที่ 3.2



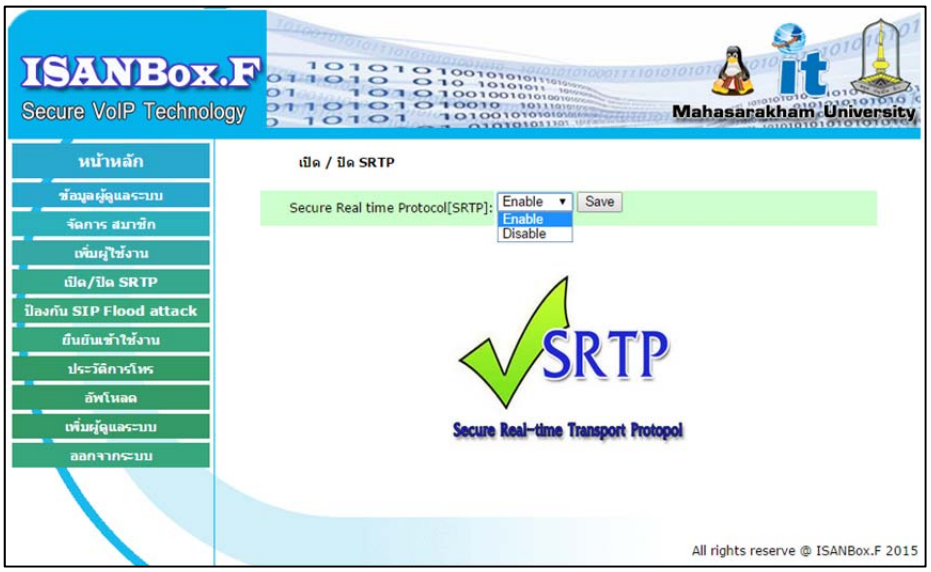
รูปที่ 3.2 โครงสร้างของระบบ ISANBox.F

ส่วนของ Web User Interface ได้มีการออกแบบแบ่งเป็น 2 ส่วน คือ ส่วนของผู้ดูแลระบบที่ใช้เพิ่ม ลบ แก้ไข ผู้ใช้งาน อัพโหลดไฟล์ ตรวจสอบการโทร จัดการระบบ กับส่วนของผู้ใช้งานที่ใช้จัดการแก้ไขข้อมูลส่วนตัว ดาวน์โหลดเอกสาร โดยระบบจะใช้งานควบคู่กับโปรแกรม PhoneLite 1.86 เนื่องจากเป็นโปรแกรมที่รองรับการทำงาน SRTP ซึ่งระบบยังสามารถใช้งานได้กับอุปกรณ์ เช่น เครื่องโทรศัพท์ IP Phone เป็นต้น ดังที่แสดงโครงสร้างการทำงานในรูปที่ 3.3



รูปที่ 3.3 โครงสร้างการทำงาน

และเนื่องจากใน FreeSWITCH จะต้องเข้าไปปรับแต่งค่าในไฟล์ XMLที่ยุ่งยาก ดังนั้นใน ISANBox.F จึงสร้างหน้าเว็บเพื่อใช้ในการเปิด/ปิดใช้งาน SRTP ดังในแสดงรูปที่ 3.4



รูปที่ 3.4 ส่วนติดต่อผู้ใช้งานที่ใช้เปิดและปิด SRTP

3.2.2 การออกแบบปรับปรุงด้านความมั่นคง ISANBox.F

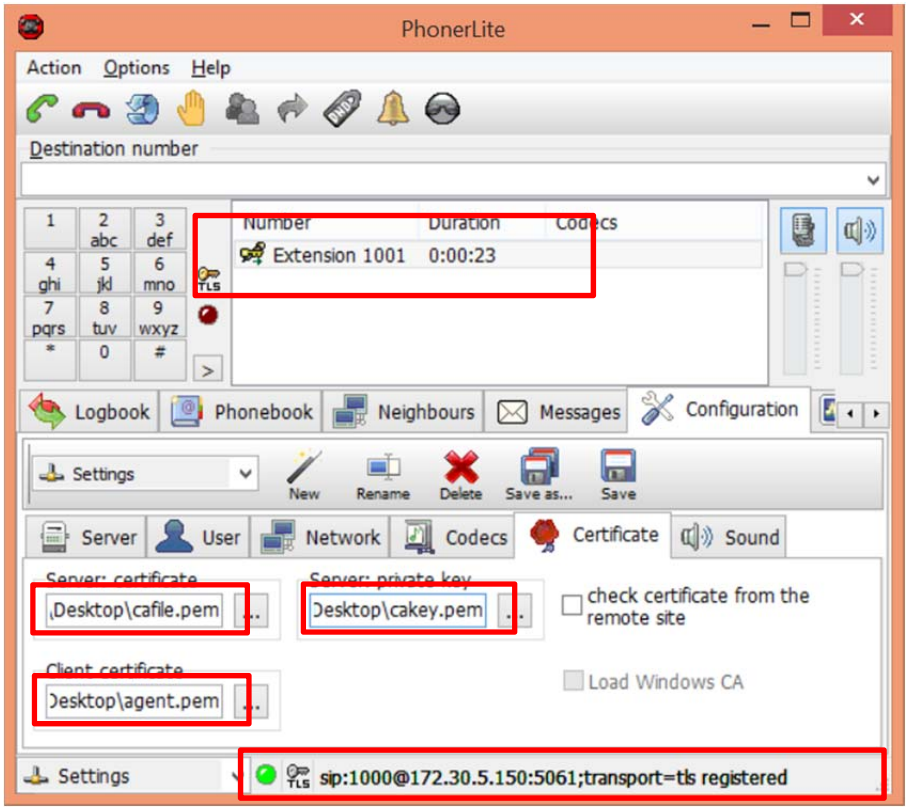
ในการออกแบบด้านความมั่นคงของระบบได้ทำการเปิดใช้งานฟังก์ชันความปลอดดภัย SIPS ที่มีใน FreeSWITCH เพื่อป้องกันการโจมตีในระดับสัญญาณ โดยการติดตั้งแพ็กเกจ libssl-dev เพื่อเปิดใช้งาน OpenSSL ลงบนระบบปฏิบัติการ CentOS จากนั้นทำการสร้าง CA (Root) Certificate ด้วยเรียกใช้ Script ดังนี้

./gentls_cert setup -cn isan.msu.ac.th -alt DNS: isan.msu.ac.th –org

เมื่อสร้าง CA (Root) เสร็จ Certificate จะถูกเก็บอยู่ใน /freeswitch/ conf/ssl/CA และสร้าง Server Certificate โดยที่เรียกใช้ Script ดังนี้

./gentls_cert create_server -cn isan.msu.ac.th -alt DNS: isan.msu.ac.th -org isan.msu.ac.th

เมื่อสร้าง Server Certificate เสร็จ Certificate จะถูกเก็บอยู่ใน /freeswitch/conf/ssl/agent.pem และสุดท้ายทำการตั้งค่านำเอา Certificate ที่สร้างขึ้นไปตั้งค่าที่ฝั่ง Client ในโปรแกรม PhonerLite ดังแสดงในรูปที่ 3.5 และรายละเอียดดังในภาคผนวก ค



รูปที่ 3.5 Configure Certificate on PhonerLite

เนื่องจากใน FreeSWITCH 1.2.6 มีฟังก์ชั่นใช้งาน SRTP ซึ่งเป็นวิธีการแก้ไขปัญหาการดักฟังเสียงการสนทนา โดยการเข้ารหัสข้อมูลเสียงก่อนส่งเข้าไปในเครือข่ายที่ใช้งานได้ผลดี งานวิทยานิพนธ์นี้จึงทำการเปิดใช้งานโพโทคอล SRTP ให้เป็นค่าเริ่มต้นของระบบ เพื่อเข้ารหัสสัญญาณเสียง โดยปรับแต่งค่าแท็ก sip_has_crypto อยู่ในไฟล์ /usr/local/freeswitch/conf/dialplan/default.xml เพื่อเปิดใช้งานโพรโทคอล SRTP ในการเข้ารหัสข้อมูลเสียงใน FreeSWITCH ดังนี้

<action application=”set” data=”sip_secure_media=true”>
<action application =”export” data=”sip_secure_media=true/”>

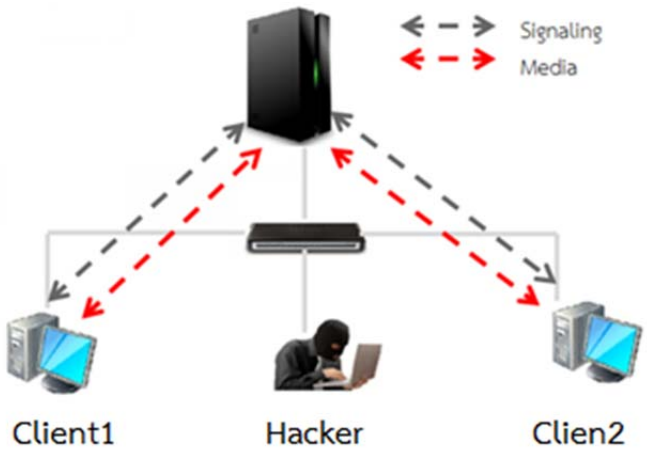
ได้พัฒนาระบบป้องกันการโจมตีแบบ SIP Flooding ซึ่งยังไม่มีใน FreeSWITCH โดยทำการตรวจสอบและวิเคราะห์ไฟล์ Log ของ FreeSWITCH ที่ /usr/local/freeswitch /log/freeswitch.log แล้วทำการเขียนโปรแกรมภาษา Shell Script เพื่อตรวจสอบหาการโจมตีในรูปแบบ SIP Flooding เมื่อพบลักษณะไฟล์ล็อกที่เป็นการจู่โจมแบบ SIP Flooding คือทั้ง Invite Flood และ Register Flood ก็ทำการสั่งงาน Iptables ให้เพิ่มกฎเพื่อบล็อกหมายเลขไอพีต้นทางของการจู่โจมที่ตรวจจับได้ ดังตัวอย่างไฟล์ล็อกการโจมตีด้วยเทคนิค SIP Flooding ของ FreeSWITCH ในรูปที่ 3.6

```
2015-02-06 15:15:17.327375 [DEBUG] sofia.c:5847 IP 192.168.1.7 Rejected by acl "domains". Falling back to Digest auth.
2015-02-06 15:15:17.334870 [DEBUG] sofia.c:5847 IP 192.168.1.7 Rejected by acl "domains". Falling back to Digest auth.
2015-02-06 15:15:17.341376 [DEBUG] sofia.c:5847 IP 192.168.1.7 Rejected by acl "domains". Falling back to Digest auth.
2015-02-06 15:15:17.347356 [DEBUG] sofia.c:5847 IP 192.168.1.7 Rejected by acl "domains". Falling back to Digest auth.
2015-02-06 15:15:17.354049 [DEBUG] sofia.c:5847 IP 192.168.1.7 Rejected by acl "domains". Falling back to Digest auth.
2015-02-06 15:15:17.358376 [DEBUG] sofia.c:5847 IP 192.168.1.7 Rejected by acl "domains". Falling back to Digest auth.
2015-02-06 15:15:17.361369 [DEBUG] sofia.c:5847 IP 192.168.1.7 Rejected by acl "domains". Falling back to Digest auth.
2015-02-06 15:15:17.368187 [DEBUG] sofia.c:5847 IP 192.168.1.7 Rejected by acl "domains". Falling back to Digest auth.
2015-02-06 15:15:17.370850 [DEBUG] sofia.c:5847 IP 192.168.1.7 Rejected by acl "domains". Falling back to Digest auth.
2015-02-06 15:15:17.381730 [DEBUG] sofia.c:5847 IP 192.168.1.7 Rejected by acl "domains". Falling back to Digest auth.
```

รูปที่ 3.6 ตัวอย่างไฟล์ Log การโจมตีด้วยเทคนิค SIP Flooding ของ FreeSWITCH

3.2.3 การทดสอบประสิทธิภาพด้านความมั่นคง ISANBox.F

วิทยานิพนธ์นี้ได้ทำการทดสอบประสิทธิภาพการให้บริการของระบบ ISANBox.F บนเครือข่ายจำลอง (Test Bed) ตามเหตุผลในหัวข้อ 3.2.3 โดยได้ออกแบบเครือข่ายเพื่อใช้ทดลองให้สามารถควบคุมปัจจัยต่างๆ ของเครือข่ายได้ ดังแสดงภาพตัวอย่างเครือข่ายในรูปที่ 3.7 และมีรายละเอียดการทดสอบดังนี้



รูปที่ 3.7 เครือข่ายการประเมินประสิทธิภาพด้านความมั่นคง

ออกแบบเครือข่าย โดยติดตั้ง ISANBox.F ทำหน้าที่เป็น VoIP Server ติดตั้งโปรแกรม Phonerlite เป็นเครื่อง Client 2 เครื่อง จากนั้น ติดตั้งเครื่องแฮ็กเกอร์ ติดตั้งระบบปฏิบัติการ Kali linux จากนั้นเชื่อมต่อเครือข่ายด้วยอุปกรณ์ Switch L2 โดยมีรายละเอียดอุปกรณ์ดังในหัวข้อที่ 3.1.2

วิทยานิพนธ์ได้ออกแบบการทดสอบ โดยทำการโจมตีระบบ ISANBox.F ด้วยเทคนิคต่างๆ บนเครือข่ายทดลองดังนี้

RTP Sniffing โจมตีเพื่อดักฟังเสียงการสนทนา โดยการใช้เทคนิคการแทรกกลางการสื่อสาสร (Man in The Middle Attack) โดยใช้โปรแกรม Cain and Abel เป็นเครื่องมือ

SIP Flooding Attack เป็นการโจมตี SIP Server โดยการทำให้เกิดการปฏิเสธการให้บริการ และระบบจะล้มเหลวและไม่ตอบสนองในที่สุด โดยใช้ Inviteflood Script ในระบบปฏิบัติการ Kali

SIP Hijacking Attack เป็นการโจมตีเพื่อดักจับ SIP Session แล้วค้นหาชื่อผู้ใช้และรหัสผ่านของโทรศัพท์ โดยใช้โปรแกรม Cain and Abel เป็นเครื่องมือ

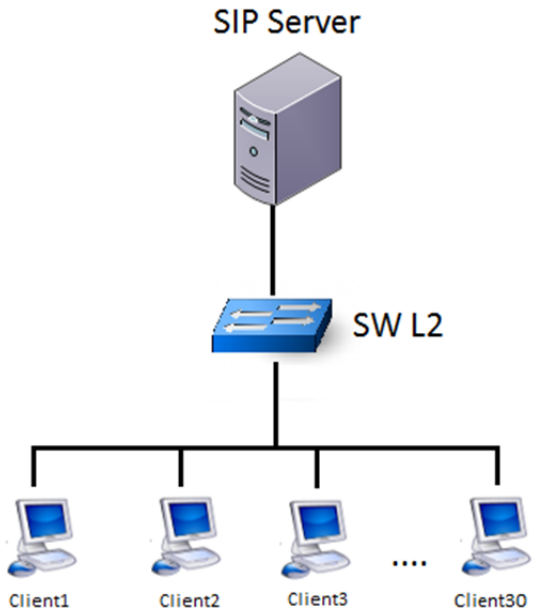
Cancel/Bye Attack เป็นการโจมตีเพื่อตัดสายในขณะที่โทรศัพท์ และสิ้นสุดการติดต่อสื่อสารโดยใช้ Teardown Script ในระบบปฏิบัติการ Kali เป็นเครื่องมือ

3.2.4 การทดสอบคุณภาพการให้บริการ ISANBox.F

วิทยานิพนธ์ได้ให้ความสำคัญเรื่องของคุณภาพการให้บริการของระบบ VoIP ที่ได้รับการเพิ่มประสิทธิภาพด้านความมั่นคง ซึ่งจากงานวิจัย งานวิจัย [12-15, 26] แสดงให้เห็นว่าการเพิ่มประสิทธิภาพความมั่นคงด้วยกระบวนการเข้ารหัสจะส่งผลกระทบต่อคุณภาพการให้บริการลดลง ดังนั้นวิทยานิพนธ์นี้จึงได้เสนอการทดสอบประสิทธิภาพ ISANBox.F ซึ่งได้ทำการประเมินคุณภาพการของระบบ ISANBox.F ว่าเป็นไปตามมาตรฐานที่กำหนดไว้หรือไม่ โดยได้ศึกษาค่าชี้วัดของคุณภาพการให้บริการ โดยที่ศึกษาจากข้อกำหนดและมาตรฐานของ ITU Telecommunication Standardization Sector (ITU-T) P.800 ได้ทดลองใช้โปรแกรมในการตรวจวัดคือโปรแกรม Commview ซึ่งสามารถใช้ตรวจวัดค่า MOS ของแพ็กเก็ตข้อมูลเสียงที่ถูกส่งผ่านเครือข่ายได้ โดยวิทยานิพนธ์นี้ได้เลือกใช้ค่า Mean Opinion Score (MOS) เป็นตัวชี้วัดถึงคุณภาพการให้บริการของระบบ ISANBox.F โดยใช้วิธีการวัดค่าแบบ E Model คือการคำนวณจากค่าปัจจัยทางด้านเครือข่าย เช่น Delay, Packet loss เป็นต้น เนื่องจากวิธีนี้เป็นวิธีที่ประหยัดต้นทุน มีความถูกต้องแม่นยำสูง อีกทั้งยังเป็นที่นิยมใช้วัดคุณภาพการให้บริการของ VoIP ในหลายๆงานวิจัย [12-15, 26] ซึ่งวิธีการคำนวณค่า MOS แบบ E Model นั้นดังที่แสดงในหัวข้อ 2.8.2 ค่า MOS จะมีระดับคะแนนตั้งแต่ 1-5 คะแนน โดยที่ คะแนน 1 คุณภาพเสียงแย่ทำให้ผู้ใช้ไม่พอใจในการใช้บริการ คะแนน 2 คือคุณภาพเสียงไม่ดีฟังเสียงได้ไม่ชัดเจน คะแนน 3 คุณภาพเสียงพอใช้อาจเสียงไม่ชัดเจนมากนักอาจจะทำให้ผู้ใช้รู้สึกหงุดหงิด คะแนน 4 คือคุณภาพเสียงดีฟังเสียงได้ชัดเจน และ คะแนน 5 คือคุณภาพเสียงยอดเยี่ยมฟังเสียงชัดเจน ดังที่แสดงในตารางที่ 2.3

จากแนวคิดดังกล่าวในขั้นต้นงานวิจัยจึงทำการลดลองติดตั้งระบบ ISANBox.F เพื่อทดลองใช้งานในเครือข่ายภายในห้องห้องปฏิบัติการคอมพิวเตอร์ จากนั้นทดลองใช้งานระบบโดยติดตั้ง Softphone จำนวน 30 ผู้ใช้งาน ไว้ภายในห้องปฏิบัติการคอมพิวเตอร์เชื่อมต่อเครือข่ายผ่านอุปกรณ์ Switch L2

ในการทดลองงานวิจัยได้เห็นถึงความสำคัญในการออกแบบการทดลองให้ถูกต้องและยุติธรรมในการทดลองให้มากที่สุด ดังนั้นงานวิจัยจึงได้เลือกวิธีและเหตุผล ที่มีความถูกต้องเหมาะสมมาใช้วัดคุณภาพการให้บริการของซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพีดังแสดงในรูปที่ 3.8

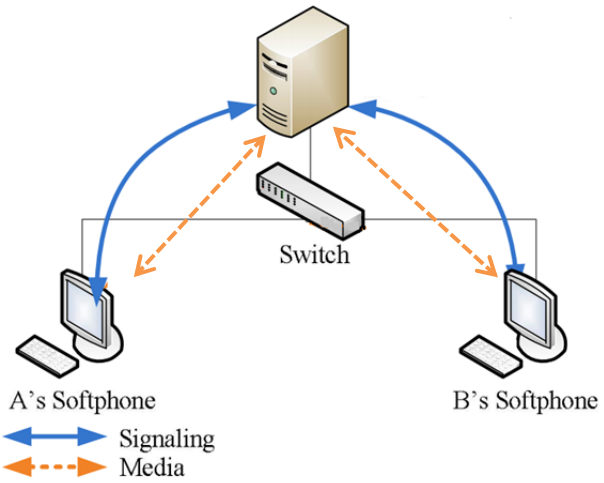


รูปที่ 3.8 แผนภาพการทดลอง

จากรูปที่ 3.8 แสดงให้เห็นแผนภาพการทดลองโดยในการทดลองวัดค่าคุณภาพการให้บริการได้ทำการทดลองในเครือข่ายระดับ LAN ซึ่งเป็นเครือข่ายภายในห้องปฏิบัติการคอมพิวเตอร์ โดยได้ออกแบบติดตั้งเครื่องให้บริการ VoIP Server เชื่อมต่อผ่าน Switch L2 และใช้เครื่องรับบริการ 30 เครื่อง (Soft phone Clients) อยู่ในห้องปฏิบัติการคอมพิวเตอร์ จากนั้นติดตั้งโปรแกรม PhonerLite เป็น Soft phone และ CommView เพื่อใช้ในการวัดค่า MOS และค่า R Factor ทำการทดลองโทรติดต่อสื่อสารกันระหว่าง Client 30 เครื่องหรือ 15 คู่สายพร้อมกัน (Concurrent Call) จำนวน 30 ครั้ง ใช้เวลาโทรครั้งละ 1 นาที ใช้ไฟล์ดนตรี Milind Date.mp3 เปิดเล่นเพลงวนไปเรื่อยๆ และตั้งค่าให้ข้อมูลเสียงผ่านช่องไมโครโฟนของโปรแกรม PhonerLite โดยทดลองโทรผ่านโพรโทคอล RTP และ SRTP ในการทดลอง ได้เลือกใช้ CODEC G.711 เพราะเป็น CODEC ที่เป็นที่นิยมในการใช้งาน เป็น CODEC ที่สามารถใช้งานได้โดยไม่มีค่าใช้จ่ายใดๆ อีกทั้งเป็น Default CODEC ของ ISANBox.F ด้วย

เพื่อให้เห็นสภาพปัญหาในบริบทของเครือข่ายที่มีความจำกัดของ Bandwidth ดังนั้นวิทยานิพนธ์นี้จึงได้เลือกวิธีจำกัด Bandwidth ที่ขาเชื่อมต่อของ VoIP โดยใช้แพ็กเก็ต Traffic Control (TC) ที่ถูกติดตั้งมาพร้อม CentOS ในการควบคุม Bandwidth 3 Mbps, 5Mbps, 10Mbps และ 100 Mbps ตามลำดับ โดยที่ Bandwidth ในฝั่งของ Client จะไม่มีปัญหาเนื่องจาก Network Interface Card ที่ใช้ทดลองสามารถลองรับ Bandwidth ที่มากพอที่จะทำให้ไม่เกิดปัญหาเรื่องของทราฟฟิกในขาเชื่อมต่อของ Client

การทดลองได้ตั้งค่าให้ข้อมูลเสียงผ่าน VoIP Server เพราะในการใช้งาน VoIP Server ในองค์กรหรือหน่วยงาน จำเป็นต้องบริหารจัดการหรือตรวจสอบการติดต่อสื่อสารของผู้ใช้งาน อาจจำเป็นต้องบันทึกการสนทนา เก็บประวัติการสนทนา หรืออาจต้องการใช้ระบบฝากข้อความเสียง ดังนั้นการทดลองจึงได้ตั้งค่าให้ข้อมูลเสียง (RTP/SRTP Streaming) วิ่งผ่าน VoIP Server ดังในรูปที่ 3.9



รูปที่ 3.9 ข้อมูลเสียงที่ไหลผ่าน VoIP Server

ในการบันทึกผลการทดลองจากกลุ่มตัวอย่างอาจจะมีความผิดพลาดหรือคาดเคลื่อน วิทยานิพนธ์นี้จึงได้ใช้ทฤษฎีแนวโน้มเข้าสู่ศูนย์กลาง (Central Limit Theorem) เพื่อใช้เก็บจำนวนกลุ่มตัวอย่างที่เหมาะสมคือทดลองกรณีละ 30 ครั้ง และได้ข้อมูลของการทดลองทั้งหมดและวิเคราะห์ข้อมูลโดยใช้ค่าสถิติคือค่าเฉลี่ย ($\bar{x}$) ดังนี้

$$\bar{x} = \frac{\sum_{i=1}^{n} x_i}{n}$$

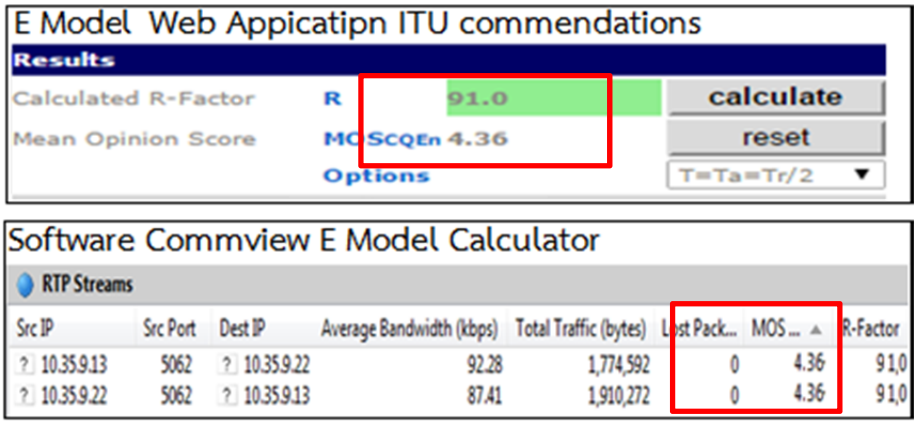
เมื่อ $\bar{x}$ แทน ค่าเฉลี่ย

$\sum x$ แทน ผลรวมของข้อมูลทั้งหมด

N แทน จำนวนข้อมูลทั้งหมด

เนื่องจากการวัดและเก็บข้อมูลจากกลุ่มตัวอย่างนั้นอาจจะมีปัจจัยอื่นที่ทำให้ผลการทดลองออกมาคาดเคลื่อน ดังนั้นวิทยานิพนธ์นี้จึงใช้การประมาณค่าเฉลี่ยของกลุ่มตัวอย่าง แบบช่วงที่ช่วงความเชื่อมั่น 95% นั่นหมายความว่าจะมีค่าผิดพลาดจากการคำนวณ 5 % คือมีระดับนัยสำคัญ (α) เท่ากับ 0.05 หรือที่ช่วงความเชื่อมั่น 95 % จากนั้นได้ทำการสรุปข้อมูลและนำเสนอในรูปแบบของตาราง และใช้กราฟในการแสดงแนวโน้มของข้อมูลให้ชัดเจนและเข้าใจง่ายยิ่งขึ้น

วิทยานิพนธ์นี้ได้ให้ความสำคัญในการเลือกใช้เครื่องมือในการทดลอง และความน่าเชื่อถือของเครื่องมือ ดังนั้นจึงได้ทำการตรวจสอบความถูกต้องของโปรแกรม Commview โดยการทดลองนำค่าปัจจัยทางด้านเครือข่าย และค่าคุณสมบัติของ CODEC ที่จำเป็นในการคำนวณตามแบบ E Model ที่ได้จากผลลัพธ์ของโปรแกรม Commview ไปตรวจสอบกับโปรแกรมคำนวณที่เป็น Web Application ขององค์กร International Telecommunication Union (ITU) ซึ่งเป็นองค์ที่รับรองมาตรฐานการวัดคุณภาพเสียงด้วยวิธี E Model โดยการทดสอบโปรแกรม Commview กับ Web Application ของทาง ITU ในเว็บไซต์ https://www.itu.int/ITU-T/studygroups/com12/emodelv1/tut.htm ผลปรากฏว่า ได้ผลลัพธ์ที่ถูกต้องและตรงกันซึ่งทำให้มั่นใจได้ว่าโปรแกรม Commview สามารถคำนวณค่าคุณภาพการให้บริการคือค่า MOS และ R Factor ได้ถูกต้องตามแบบที่มาตรฐานที่ ITU กำหนด ดังแสดงตัวอย่างการตรวจสอบในรูปที่ 3.10



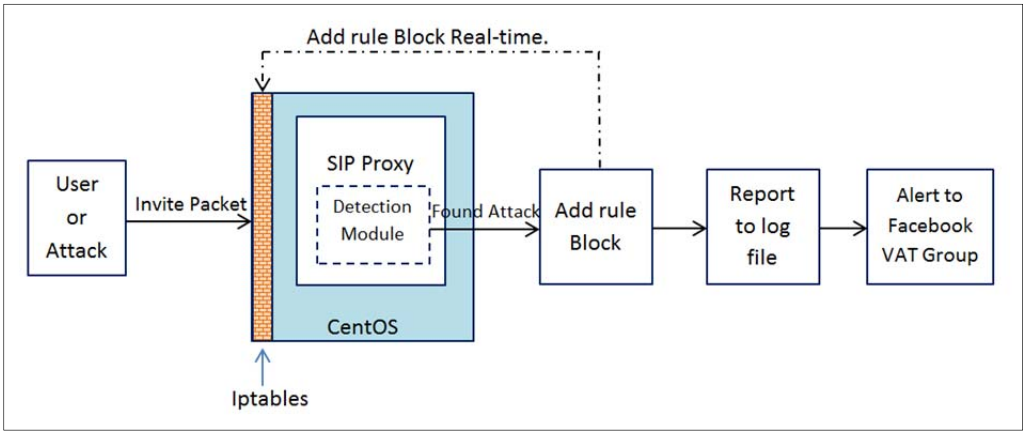
รูปที่ 3.10 ตรวจสอบความถูกต้องโปรแกรม Commview กับ E Model Web Application ITU

3.2.5 การทดสอบประสิทธิภาพส่วนติดตั้งและส่วนติดต่อผู้ใช้งาน

วิทยานิพนธ์นี้ได้ให้ความสำคัญด้านการพัฒนาส่วนติดต่อผู้ใช้งานของระบบ ISANBox.F โดยที่ได้พัฒนาส่วนติดต่อผู้ใช้งานและส่วนการติดตั้ง เพื่อให้ผู้ใช้งานทั่วไปสามารถติดตั้งและใช้งานระบบได้อย่างสะดวก และง่ายต่อการนำระบบ ISANBox.F ไปใช้งาน ดังนั้นหลังจากที่ได้พัฒนาส่วนติดต่อผู้ใช้งานและส่วนติดตั้งแล้ว จึงได้ทำการทดสอบประสิทธิภาพของส่วนติดตั้งและส่วนติดต่อผู้ใช้งาน โดยเลือกใช้วิธี Keystroke-Level Model (KLM) ตามในหัวข้อที่ 2.9.6 เพื่อใช้วัดเวลาในการใช้งานของส่วนติดต่อผู้ใช้งานและการติดตั้งระบบ โดยจำทดสอบเปรียบเทียบระหว่าง การติดตั้งและใช้งาน FreeSWITCH แบบเดิม และการติดตั้งใช้งาน ISANBox.F

3.3 ออกแบบแนวทางแก้ไขปัญหา SIP Flooding

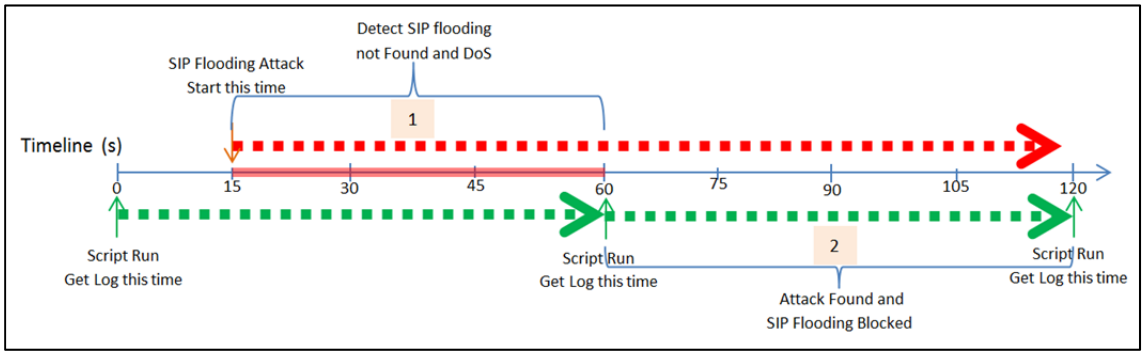
จากการพัฒนาปรับปรุงประสิทธิภาพด้านความมั่นคงของซอฟต์แวร์ FreeSWITCH นั่น จากผลการทดสอบประสิทธิภาพด้านความมั่นคงในเชิงลึก ยังพบประเด็นที่เป็นปัญหาเพิ่มเติมนั่นคือ การแก้ไขปัญหา SIP Flooding นั้นยังพบความไม่สมบูรณ์ในการใช้เทคนิคการอ่านไฟล์ Log เพื่อตรวจสอบการโจมตี ทำให้เกิดการตอบสนองต่อการโจมตีไม่ทันเหตุการณ์ วิทยานิพนธ์นี้จึงได้เสนอแนวคิดการออกแบบแก้ไขปัญหาการโจมตีด้วยเทคนิค SIP Flooding โดยมีการตรวจจับการโจมตีได้ทันต่อเหตุการณ์คือวิเคราะห์พฤติกรรมข้อความตอบสนอง (Response Message) ที่เกิดจากการตอบกลับของข้อความ Invite ต่อจากนั้นทำการวิเคราะห์และระบุต้นทางการโจมตีของผู้ไม่หวังดีแล้วเพิ่มกฎใน Iptables ให้บล็อกการโจมตีทันที สุดท้ายเสนอให้มีระบบออกรายงานการโจมตีไปที่ไฟล์ Log ของระบบและการแจ้งเตือนในกลุ่ม Facebook ของผู้ดูแลระบบ VoIP Admin Team (VAT) ซึ่งได้เสนอแนวคิดการแก้ไขปัญหาดังในรูปที่ 3.11



รูปที่ 3.11 แนวการแก้ไขปัญหา SIP Flooding แบบที่ตอบสนองทันต่อการโจมตี

3.3.1 วิเคราะห์ปัญหาการป้องกัน SIP Flooding โดยการใช้ไฟล์ Log เพื่อตรวจสอบการโจมตีงานวิจัยนี้ได้ทำการทดลองโจมตี SIP Flooding ในระบบที่มีการป้อกันการโจมตีด้วยวิธีการอ่านไฟล์ Log เพื่อตรวจหาการโจมตี เช่นในงานวิจัย [7] หรือใน ระบบ ISANBox.F ที่ได้พัฒนาขึ้นในวิทยานิพนธ์นี้ โดยผลการทดลองพบว่ายังมีบางช่วงเวลาที่เป็น Script ยังไม่ถึงรอบเวลาการทำงาน จึงไม่สามารถตรวจจับและป้องกันการโจมตีได้ทันเวลา ซึ่งสามารถวิเคราะห์ปัญหาการป้องกันการโจมตีด้วยการอ่านไฟล์ Log ได้ดังนี้

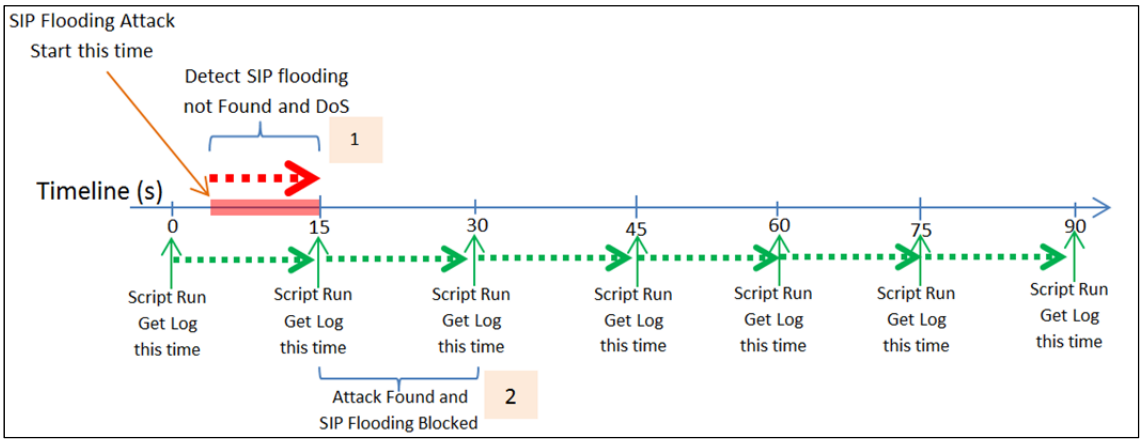
ถ้าตั้งเวลาให้ Script ทำงานทุกๆ 1 นาที ถ้าหากการโจมตีเกิดขึ้นหลังจากที่ Script ทำงานไป 15 วินาทีแรก การโจมตีครั้งนั้นก็จะไม่ถูกตรวจจับในการทำงานของ Script รอบนั้น แต่จะถูกตรวจจับและบล็อกการโจมตีในรอบ 1 นาทีถัดไป โดยจะมีเวลาที่โดนโจมตีแล้วไม่ถูกตรวจจับถึง 45 วินาที ซึ่งก็เป็นการแก้ปัญหาที่ไม่สมบูรณ์ และจะส่งผลให้เกิดการปฏิเสธการให้บริการของ SIP Proxy ได้ในที่สุด ดังแสดงรูปแบบการแก้ไขปัญหาที่ไม่สมบูรณ์ของการใช้ Srcipt อ่านไฟล์ Log ในรูปที่ 3.12



รูปที่ 3.12 ความไม่สมบูรณ์ของการแก้ไขปัญหา SIP Flooding ด้วยการอ่านไฟล์ Log

ในทางตรงกันข้ามถ้าหากมีการปรับวงรอบการทำงานของ Script ให้มีความถี่มากขึ้น เพื่อให้มีการตอบสนองต่อการโจมตีได้รวดเร็วขึ้น เช่น ตั้งเวลาให้ Script ทำงานอ่านไฟล์ Log เพื่อตรวจสอบการโจมตีในทุกๆ 15 วินาทีสิ่งที่เกิดขึ้นคือ จะเกิดการ Self-Flooding นั่นหมายถึงจะมีโพรเซสของ Script ที่ใช้ตรวจจับเกิดขึ้นทุก 15 วินาที ทำให้ระบบเกิดภาระงานที่เพิ่มสูงมากขึ้น และมีการใช้ทรัพยากรของระบบมากขึ้นตามมาด้วย ซึ่งจะทำให้เกิดการปฏิเสธการให้บริการได้เช่นกัน อีกทั้งยังเกิดช่วงเวลาที่ Script ตรวจไม่พบการโจมตี เช่น ถ้าหากการโจมตีเกิดขึ้นหลังจากที่ Script เพิ่งทำงานไป 5 วินาทีแรก การโจมตีครั้งนั้นก็จะไม่ถูกตรวจจับในการทำงานของ Script รอบนั้น แต่จะถูกตรวจจับและบล็อกการโจมตีในรอบ 15 วินาทีถัดไป ซึ่งยังมีช่วงเวลาที่ถูกโจมตีแต่ไม่ถูกตรวจจับถึง 10 วินาที ดังแสดงรูปแบบการเพิ่มความถี่ในการทำงานของ Script ในการตรวจหาการโจมตีในรูปที่ 3.13

ถ้าหากนำระบบป้องกัน SIP Flooding โดยการตรวจสอบการโจมตีจากไฟล์ Log ไปใช้ในทางธุรกิจที่มีความวิกฤตในการติดต่อสื่อสารสูง หรือธุรกิจที่มีความเข้มงวดในเรื่องความเสถียรของระบบ ก็อาจจะเกิดความเสียหายให้กับองค์กรหรือธุรกิจนั้นได้เช่นกัน



รูปที่ 3.13 รูปแบบการทำงานของ Script เมื่อเพิ่มความถี่ในการทำงาน

วิทยานิพนธ์นี้ได้ทำการทดลองเพิ่มเติมเพื่อแสดงให้เห็นถึงปัญหาของการแก้ปัญหา SIP Flooding ด้วยวิธีการอ่านไฟล์ Log ที่มีการตอบสนองไม่ทันต่อการโจมตี โดยได้พัฒนา SIP Proxy ต้นแบบ แล้วใช้ Script ในการอ่านไฟล์ Log เพื่อตรวจจับการโจมตี ซึ่งได้ออกแบบการทดลองและมีผลการทดลองดังนี้

1) ออกแบบการทดลอง

1. ตั้งค่าเวลาการทำงานของ Script ที่ตรวจจับการโจมตีให้ทำงานทุกๆ 30 วินาที

2. แบ่งการทดลองเป็น 2 กรณีคือ กรณีที่ตอบสนองได้เร็วที่สุด และกรณีที่ตอบสนองได้ช้าที่สุด

กรณีตอบสนองเร็วที่สุด คือ ทำการโจมตีก่อนที่ Script ทำงาน 1 วินาที

กรณีตอบสนองช้าที่สุด คือ ทำการโจมตีหลังจาก Script ทำงาน 1 วินาที

3. ใช้ Inviteflood Script ในระบบปฏิบัติการ Kali Linux โจมตีด้วยการส่งข้อความ Invite ไปยัง SIP Proxy ในอัตราเร็ว 50000 แพ็กเก็ตต่อวินาที

4. ทดลองกรณีละ 30 ครั้ง บันทึกผล ใช้ค่าเฉลี่ยของเวลา ที่ช่วงความเชื่อมั่น 95 %

5. ติดตั้งเครือข่ายทดลองแบบ Test-beds ตามหัวข้อ 2.9.7

2) ผลการทดลอง

โดยปกติการที่ Script จะตรวจพบการโจมตีในไฟล์ Log ได้นั้น ก็จะเกิดขึ้นหลังจากที่เกิดการโจมตีขึ้นแล้ว จึงจะปรากฏประวัติการโจมตีในไฟล์ Log ของ SIP Proxy ดังนั้นถึงแม้จะอยู่ในกรณีที่ตอบสนองการโจมตีได้เร็วที่สุดก็ยังคงมีความล่าช้าอยู่พอสมควรดังจะเห็นได้จากผลการทดลองดังนี้

ตารางที่ 3.1 การตอบสนองการโจมตีของการแก้ปัญหา SIP Flooding ด้วยการอ่านไฟล์ Log

กรณีที่ตอบสนอง	เวลาที่ใช้ในการตอบสนอง (วินาที)
กรณีตอบสนองเร็วที่สุด	9.11 ± 0.10
กรณีตอบสนองช้าที่สุด	38.09 ± 0.13

จากตารางที่ 3.1 พบว่าผลการทดลองในกรณีที่ตอบสนองเร็วที่สุดก็ยังใช้เวลาในการตอบสนองถึง 9.11 ± 0.10 วินาที และในกรณีที่ตอบสนองช้าที่สุดที่เป็นไปได้ จะใช้เวลาในการตอบสนองนานถึง 38.09 ± 0.13 วินาที ระยะเวลาดังกล่าวนี้ SIP Proxy จะโดนโจมตีโดยการส่งข้อความ Invite มายัง SIP Proxy ในอัตราที่เร็วถึง 50000 ข้อความต่อวินาที ซึ่งเป็นเวลาที่นานพอที่จะทำให้ระบบ VoIP ไม่ตอบสนองผู้ใช้งาน และทำให้ระบบล้มเหลวลงในที่สุด

ซึ่งการป้องกัน SIP Flooding แบบอ่านและวิเคราะห์ไฟล์ Log จะแตกต่างกับวิธีที่เสนอในงานวิทยานิพนธ์นี้ซึ่งจะทำงานตอบสนองการโจมตีได้ดีและทันเหตุการณ์มากกว่าแบบอ่านไฟล์ Log เนื่องจากส่วนการตรวจจับการโจมตีตามวิทยานิพนธ์นี้ ได้ออกแบบให้ติดอยู่กับโครงสร้างของโพรโทคอล SIP นั่นหมายความว่า ถ้าหาก SIP Proxy ไม่ได้รับข้อความ Invite ส่วนการตรวจจับนี้ก็จะไม่ทำงานให้สิ้นเปลืองทรัพยากรของระบบ แต่ถ้ามีการได้รับข้อความ Invite จากผู้ใช้ปกติที่ไม่ใช่การโจมตี ส่วนการตรวจจับนี้ก็จะไม่กระทำกระบวนการอื่นใดต่อ แต่ถ้าหากเมื่อไหร่ที่มีการโจมตีเข้ามาที่ SIP Proxy ส่วนการตรวจจับนี้ก็จะทำงานตรวจจับโดยทันทีและจะส่งต่อสู่กระบวนการบล็อกการโจมตี การออกรายงานสู่ไฟล์ Log และวิทยานิพนธ์นี้ยังได้เสนอระบบการแจ้งเตือนไปยังกลุ่ม VoIP Administrator Team ใน Facebook ทำให้ผู้ดูแลระบบที่อยู่ในกลุ่มได้รับการแจ้งเตือนการโจมเตือนการโจมตีอย่างรวดเร็วและทั่วถึง

3.3.2 การตรวจวิเคราะห์ Response Message เพื่อตรวจจับการโจมตี

จากตัวอย่าง Response Message ในรูปที่ 3.14 เป็นการตอบกลับเพื่อร้องขอการยืนยันตัวตนจากต้นทาง (Proxy Authentication required) ซึ่งต้นทางจะไม่มีการยืนยันตัวตนกลับมา แต่จะส่ง Invite Message แบบเดิมมาซ้ำๆเป็นจำนวนมากในอัตราเร็วที่มากกว่าปกติ ดังนั้นจึงปรากฏพฤติกรรมของ Response Message ในข้างต้น ที่มีข้อความร้องขอให้ยืนยันตัวตนจาก SIP Proxy เช่น “407 Proxy Authentication required” และ From Tag เช่น “From: <sip:192.168.1.7:9>”

```
SIP/2.0 407 Proxy Authentication required
Via: SIP/2.0/UDP 192.168.1.7:9;branch=bd5a9e75-8746-4554-a0ca-
e10000000002
To: "1000" <sip:1000@192.168.1.4:5060>
From: <sip:192.168.1.7:9>;tag=bd5aa906-8746-4554-a8ea-bc0000000002
Call-ID: bd5ab266-8746-4554-a856-da0000000002
CSeq: 2 INVITE
Proxy-Authenticate: Digest
nonce="3b284e2a411a35089190bae87f84a9dc",realm="nist.gov",opaque="",stale
=FALSE,algorithm=MD5
Content-Length: 0
```

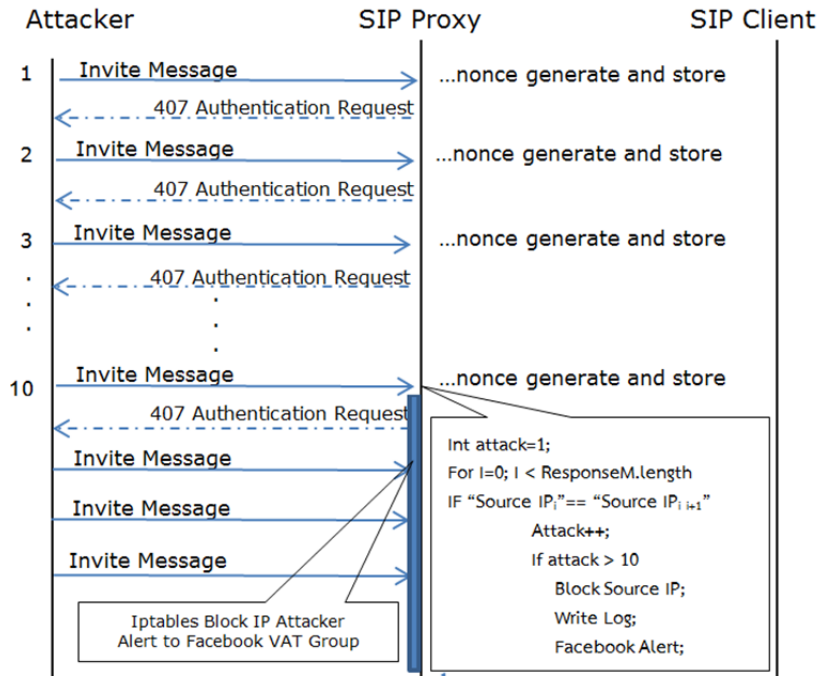
รูปที่ 3.14 Response Message ที่เกิดจากการตอบข้อความ Invite ของ SIP Proxy

3.3.3 การเลือกใช้ค่าขีดแบ่ง (Threshold) ในการจำแนกการโจมตี

วิทยานิพนธ์นี้ได้ให้ความสำคัญเรื่องค่าขีดแบ่ง (Threshold) ที่เหมาะสม สำหรับการจำแนกรูปแบบข้อความ Invite ว่าเซสชั่นใดเป็นการร้องขอใช้งานแบบปกติหรือเซสชั่นใดเป็นการร้องขอในรูปแบบการโจมตีแบบ SIP Flooding เพื่อลดความผิดพลาดในการตรวจจับการโจมตี ซึ่งวิทยานิพนธ์นี้ได้ทำการศึกษาถึงพฤติกรรมที่เป็นไปได้ของลักษณะการโจมตี พบว่าลักษณะของแพ็กเก็ตจะถูกส่งจากแหล่งต้นทางเดียวกันติดต่อกันในอัตราที่สูงกกว่าการ้องขอใช้งานปกติ ซึ่งผู้ใช้งานโดยทั่วไปจะไม่สามารถส่งข้อความ Invite ผ่านทางโปรแกรมประเภท SIP Client จากผู้ใช้รายเดิมติดต่อกันเพื่อร้องขอการสร้างเซสชั่นสื่อสารได้ถึง 10 ครั้งภายในเวลา 1 วินาที

และเมื่อพิจารณาถึงความเป็นไปได้ที่จะเกิดความผิดพลาดในการส่งข้อความ Invite ไปยัง SIP Proxy แล้วข้อความนั้นไปไม่ถึง ซึ่งเป็นไปได้ที่ข้อความ Invite นั้นจะเกิดการสูญหายขึ้นในเครือข่ายจากเหตุต่างๆ ดังนั้นถ้าหากมีการใช้โพรโทคอล SIP บน โพรโทคอล TCP ก็จะทำให้กลไกการทำงานของโพรโทคอล TCP ทำการส่งข้อความ Invite ซ้ำไปเรื่อยๆ จนกว่าจะส่งข้อความ Invite สำเร็จ และเมื่อพิจารณาถึงจำนวนครั้งที่เป็นไปได้ในการส่งข้อความ Invite ซ้ำในกรณีนี้พบว่า เมื่อเทียบกับค่าเวลาตอบสนอง (Response Time) โดยเฉลี่ยของเครือข่ายภาพรวมทั้งโลกอยู่ที่ 94 มิลลิวินาที [44] (ข้อมูลจากเว็บไซต์ Internet Traffic Report เมื่อวันที่ 29 พฤษภาคม พ.ศ. 2558) นั่นหมายถึงในสถานการณ์จริง ถ้าหากมีการส่งข้อความซ้ำที่เกิดจากกลไกการทำงานของโพรโทคอล SIP ที่มีสาเหตุจากการส่งข้อความ Invite ไปไม่ถึง SIP Proxy ดังนั้นภายใน 1 วินาที (1000 มิลลินาที) จะส่งข้อความซ้ำได้ไม่เกิน 10 ครั้ง ซึ่งถ้าหากมีการส่งข้อความซ้ำเกินกว่า 10 ครั้งในเวลา 1 วินาที ก็เป็นไปได้ว่าการส่งข้อความนั้นเป็นการโจมตีแบบ SIP Flooding

ดังนั้นวิทยานิพนธ์นี้นี้จึงพิจารณาเห็นควรเลือกใช้ค่า 10 เป็นค่าขีดแบ่งในการจำแนกการโจมตี นั่นหมายความว่าถ้ามีการส่งข้อความ Invite มาจากต้นทางเดิมติดต่อกันอย่างต่อเนื่อง 10 ข้อความภายใน 1 วินาที ให้ถือว่าเซสชั่นนั่นคือการโจมตี ดังแสดงลักษณะการวิเคราะห์การโจมตีดังในรูปที่ 3.15



รูปที่ 3.15 การวิเคราะห์การโจมตี SIP Flooding จาก Response Message

รูปที่ 3.15 แสดงให้เห็นถึงการวิเคราะห์การโจมตี SIP Flooding จาก Response Message คือเมื่อ Attacker ส่งข้อความ Invite มาที่ SIP Proxy ตั้งแต่ข้อความแรก จะมีการตรวจสอบต้นทางการส่งข้อความ และประเภทของข้อความ ถ้าหากส่งข้อความซ้ำจากต้นทางเดิมถึง 10 ครั้งอย่างต่อเนื่องใน 1 วินาที ส่วนการตรวจจับจะประมวลผลและสั่งให้ iptables ทำการเพิ่มกฎเพื่อบล็อก

ข้อความ Invite จาก Attacker โดยทันที จากนั้นจะทำการบันทึกประวัติการโจมตีไปที่ไฟล์ Log ของ SIP Proxy และทำการแจ้งเตือนใน Facebook กลุ่มผู้ดูแลระบบ VoIP

3.3.4 การพัฒนา SIP Proxy ต้นแบบ

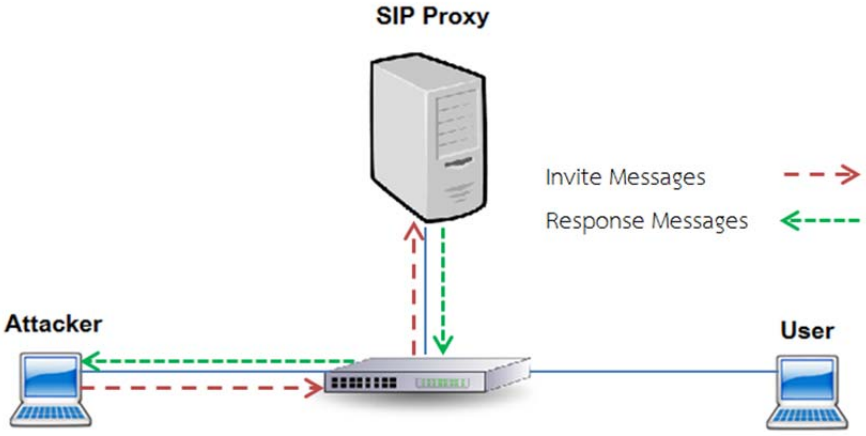
วิทยานิพนธ์นี้ได้การพัฒนาซอฟต์แวร์ SIP Proxy ต้นแบบเพื่อใช้ในการทดสอบประสิทธิภาพของแนวคิดที่ได้เสนอแก้ไขปัญหา SIP Flooding โดยเลือกใช้ Jain-SIP ซึ่งเป็น Java API ที่ใช้จัดการ Signaling Protocol และสร้าง SIP Stack ตามที่มาตรฐาน SIP (RFC 3261) กำหนด โดยวิทยานิพนธ์นี้ พัฒนาส่วนการตรวจจับการโจมตีเพิ่มเข้าไปโครงสร้างของโพรโทคอล SIP โดยได้พัฒนาต่อยอดเข้าไปในคลาส Proxy ในเมธทอด processInvite ดังตัวอย่างโค๊ดโปรแกรมในผนวก ง

วิทยานิพนธ์นี้ได้ให้ความสำคัญกับเรื่องการรายงานและแจ้งเตือนการโจมตี SIP Flooding เนื่องจากทุกการโจมตีที่เกิดขึ้นกับระบบเครือข่ายนั้น จำเป็นอย่างยิ่งที่ผู้ดูแลระบบจะต้องรับทราบและเข้าถึงข้อมูลการโจมตี เพื่อใช้ในการวิเคราะห์ วางแผนจัดการและแก้ไขปัญหาต่อไป ซึ่งการแจ้งเตือนนั้นก็จำเป็นจะต้องทันต่อเหตุการณ์ และหากในกรณีที่มีผู้ดูแลระบบหลายคนก็จำเป็นอย่างยิ่งที่การแจ้งเตือนนั้นจะเข้าถึงผู้ดูแลระบบทุกคนอย่างทั่วถึง ด้วยเหตุนี้วิทยานิพนธ์จึงนำเอาระบบของโซเชียลมีเดีย โดยเลือกใช้ Facebook เนื่องจากเป็นที่นิยมใช้งานกันอย่างแพร่หลายและไม่มีค่าใช้จ่ายในการดำเนินการ เข้ามาประยุกต์ใช้งานในการแจ้งเตือนการโจมตี โดยได้พัฒนาต้นแบบระบบแจ้งเตือนการโจมตีไปยังกลุ่ม Facebook เนื่องจากสมาชิกในกลุ่มนี้จะมีเพียงผู้ดูแลระบบที่เกี่ยวข้องเท่านั้น และกลุ่มนี้จะใช้วัตถุประสงค์ในการแจ้งแจ้งเตือนการโจมตี และแลกเปลี่ยนข้อมูลที่เป็นประโยชน์กับระบบเครือข่าย ดังนั้นจึงได้ตั้งค่ากลุ่ม Facebook ของผู้ดูแลระบบ VoIP นี้ให้เป็นแบบกลุ่มลับ ซึ่งพัฒนาโดยใช้ Facebook API [42] ด้วยภาษา PHP เป็นฐานในการพัฒนา ทำการสร้าง Application ใน Facebook ชื่อ SIP Flooding Detect ซึ่งเมื่อ SIP Proxy ตรวจพบการโจมตีก็จะเรียกใช้ Facebook API ให้ใช้สิทธิในการเข้าถึงกระดานของกลุ่มผู้ดูแลระบบ VoIP แล้วโพสต์ข้อความแจ้งเตือน ดังแสดงตัวอย่างการ Application บน Facebook ในรูปที่ 3.16 สุดท้ายได้พัฒนาระบบรายงานการโจมตี โดยทำการบันทึกประวัติการโจมตีไปยังไฟล์ sipflooding.log ของ SIP Proxy ต้นแบบ

รูปที่ 3.16 ตัวอย่างการสร้าง Application บน Facebook

3.3.5 การทดสอบประสิทธิภาพ SIP Proxy ต้นแบบ

วิทยานิพนธ์นี้ได้เลือกใช้เครือข่ายในการทดสอบประสิทธิภาพด้านความมั่นคงเป็นแบบเครือข่ายจำลอง (Test Bed) ตามเหตุผลในหัวข้อ 3.1.3 ดังแสดงตัวอย่างเครือข่ายการทดลองดังที่แสดงในรูปที่ 3.17 เป็นการติดตั้งเครือข่ายการทดลอง เชื่อต่อเครือข่ายด้วยอุปกรณ์ Switch L2 ซึ่งได้ติดตั้งระบบปฏิบัติการ Kali Linux บนเครื่องของ Attacker จากนั้นพัฒนาโปรแกรมต้นแบบจาก Jain-SIP Java API ซึ่งทำหน้าที่เป็น SIP Proxy ทำงานได้ตามมาตรฐานของโพรโทคอล SIP จากนั้นเชื่อมต่อเครื่องผู้ใช้ทั่วไปอีก 1 เครื่องเข้าไปในเครือข่าย โดยจะทดสอบประสิทธิภาพกับทั้ง SIP Proxy ที่ไม่มีการป้องกันและ SIP Proxy ต้นแบบที่การป้องกัน SIP Flooding



รูปที่ 3.17 รูปแบบเครือข่ายการทดลอง

ในการทดลองเพื่อวิเคราะห์ปัญหาและผลกระทบที่เกิดขึ้นกับ SIP Proxy เมื่อถูกโจมตีด้วยเทคนิค SIP Flooding การทดลองนี้ได้กำหนดตัวชี้วัดไว้ดังนี้

1. การทำงานของหน่วยประมวลผล การทำงานของหน่วยประมวลผลกลาง CPU โดยทำการประเมินร้อยละของการทำงานทั้งหมดของหน่วยประมวลผลกลางและการฟื้นตัวหลังการจู่โจม

2. การใช้งานหน่วยความจำ (Memory Usage) โดยทำการประเมินผลร้อยละของการใช้งานทั้งหมดของหน่วยความจำที่ใช้งาน

3. เวลาในการตอบสนองการโจมตี โดยเริ่มตั้งแต่เวลาที่เริ่มทำการโจมตีจนถึงเวลาที่ SIP Proxy ต้นแบบ ตรวจจับพบการโจมตี

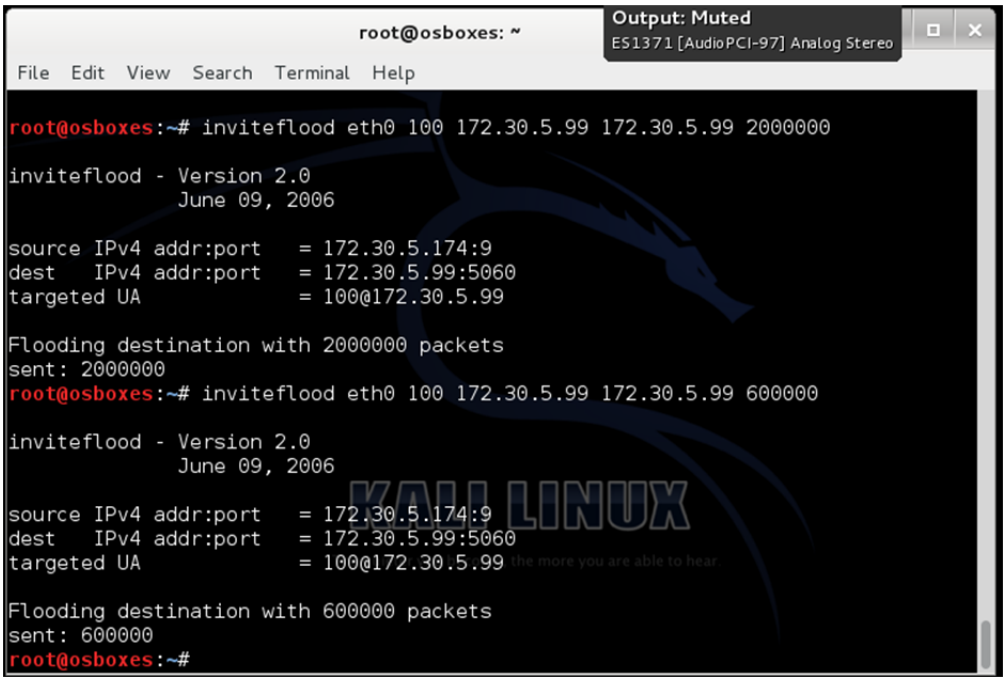
ตารางที่ 3.2 รูปแบบข้อมูลการจู่โจม SIP Flooding

Content	Time	Invite Message
ก่อนจู่โจม	30 วินาที	-
ขณะที่จู่โจม	60 วินาที	50000*60
หลังการจู่โจม	120 นาที	-
หลังการจู่โจม	+30 วินาที (วินาทีที่ 120-150)	

ทำการทดสอบประสิทธิภาพเปรียบเทียบระหว่าง SIP Proxy แบบที่ไม่มีการป้องกัน SIP Flooding และ SIP Proxy ต้นแบบที่ใช้แนวทางการแก้ปัญหาตามที่เสนอในวิทยานิพนธ์โดยใช้ระบบปฏิบัติการ Kali Linux ทำการส่งข้อความ INVITE ให้กับ SIP Proxy ดังตัวอย่างในรูปที่ 3.18 ในอัตราความเร็วเฉลี่ยประมาณ 50000 Packets ต่อวินาทีดังข้อมูลในตารางที่ 3.2 เก็บข้อมูลการใช้งานของหน่วยประมวลผลกลางและหน่วยความจำ ตั้งแต่เริ่มการจู่โจมและสิ้นสุดการจู่โจม เพื่อดูผลกระทบที่เกิดขึ้น เก็บข้อมูลการทำงานหน่วยประมวลผลกลางและ หน่วยความจำ ทุกๆ 1 วินาที โดยแบ่งเป็น 4 ช่วงเวลา ได้แก่ ก่อนทำการจู่โจม 30 วินาที ขณะจู่โจม 60 วินาที หลังการจู่โจม 120 วินาที และช่วงเวลาหลังการโจมตีเพิ่มอีก 30 วินาที (วินาทีที่ 210-240 ของการโจมตี) ทำการทดลอง 30 ครั้ง บันทึกข้อมูลด้วยโปรแกรม Excel ใช้ข้อมูลผลการทดลองโดยเฉลี่ย ($\overline{X}$) ที่ระดับความเชื่อมั่น 95% ดังแสดงตัวอย่างการโจมตีด้วยชุดคำสั่ง Invite Flood ซึ่งมีรายละเอียดดังนี้

Inviteflood eth0 1000 172.30.5.74 172.30.5.74 600000

Inviteflood	คำสั่งเรียกใช้และให้ Run Script ชื่อ Inviteflood
eth0	ชื่อ Interface
1000	ชื่อผู้ใช้เป้าหมาย
172.30.5.74	หมายเลขไอพี SIP Proxy เป้าหมาย
172.30.5.74	หมายเลขไอพี ผู้ใช้ เป้าหมาย
600000	จำนวน Packet ที่ Flood ไปยังเป้าหมาย



รูปที่ 3.18 ภาพการโจมตี SIP Flooding ด้วย Kali Linux

บทที่ 4

ผลการวิจัยและการอภิปราย

ในบทนี้จะได้กล่าวถึงผลการพัฒนาระบบ ISANBox.F และการออกแบบแนวทางแก้ไขปัญหา SIP Flooding ที่ได้ทำการทดลองและพัฒนาไปในบทที่ 3 ซึ่งได้แบ่งผลการทดลองและพัฒนาออกเป็น 2 ส่วนหลักๆ ดังต่อไปนี้

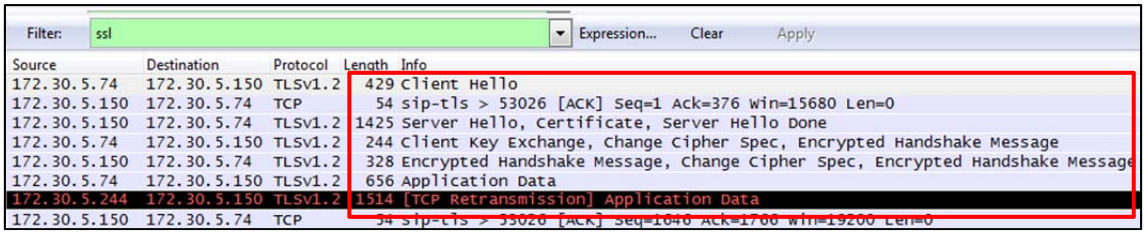
4.1 ผลการพัฒนาระบบ ISANBox.F

4.1.1 ผลการทดสอบทางด้านความมั่นคง

งานวิจัยได้ทดสอบประสิทธิภาพด้านความมั่นคงของ ISANBox.F โดยได้ผลการทดสอบประสิทธิภาพด้านความมั่นคงดังนี้

1) การโจมตี SIP Register Hijacking

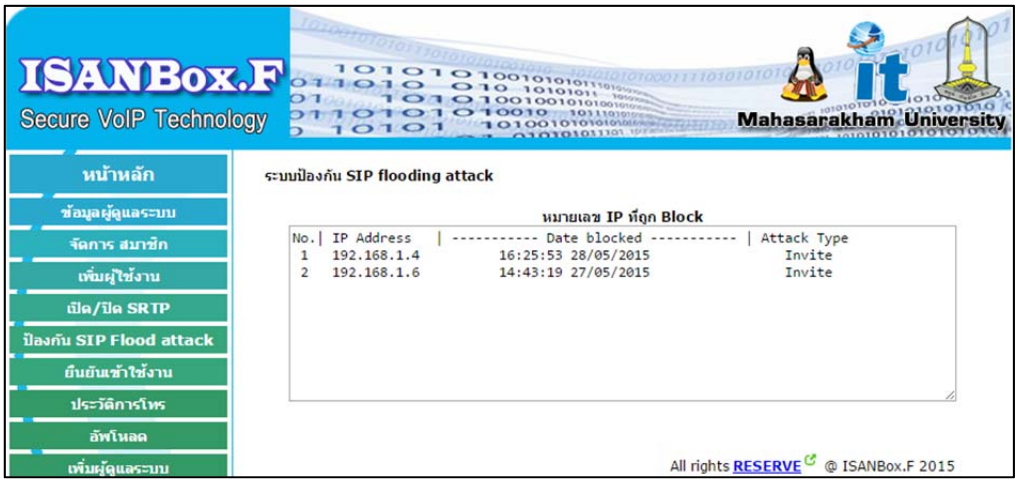
การโจมตี SIP Register Hijacking ด้วยโปรแกรม Cain & Abel โจมตีเพื่อดักจับค้นหาชื่อผู้ใช้และรหัสผ่านของหัวโทรศัพท์ จาก SIP Register Session ผลปรากฏว่า ไม่สามารถดักจับ SIP Session แล้วค้นหา User และ Password ของผู้ใช้ได้ เนื่องจากมีการเปิดใช้โพรโทคอล SSL (SIPS) เพื่อเข้ารหัสช่องสัญญาณ ดังแสดงในตัวอย่างการใช้จากโปรแกรม Wireshark ในรูปที่ 4.1



รูปที่ 4.1 การใช้งานโพรโทคอล TLS (SIPS)

2) การโจมตี SIP Flooding

การโจมตี SIP Flooding โดยใช้ชุดคำสั่ง Invite ใน Kali Linux เพื่อทำให้ระบบ VoIP เกิดการปฏิเสธการให้บริการต่อผู้ใช้ ปรากฏว่าจะไม่เกิดการปฏิเสธการให้บริการของระบบ ISANBox.F เนื่องจากมี Script ที่ใช้วิเคราะห์และตรวจสอบล็อกไฟล์แล้วสั่ง Iptables ให้บล็อกไอพีต้นทางของการ Flood แต่มีเพียงบางช่วงเวลาที่ Script ทำงานไม่ตอบสนองต่อการโจมตีได้อย่างทันเวลาจึงยังถูกโจมตีด้วยเทคนิคนี้ได้เป็นช่วงเวลาสั้นๆ ดังแสดงตัวอย่างการ Block หมายเลขไอพีต้นทางที่แสดงทาง Web User Interface ในรูปที่ 4.2



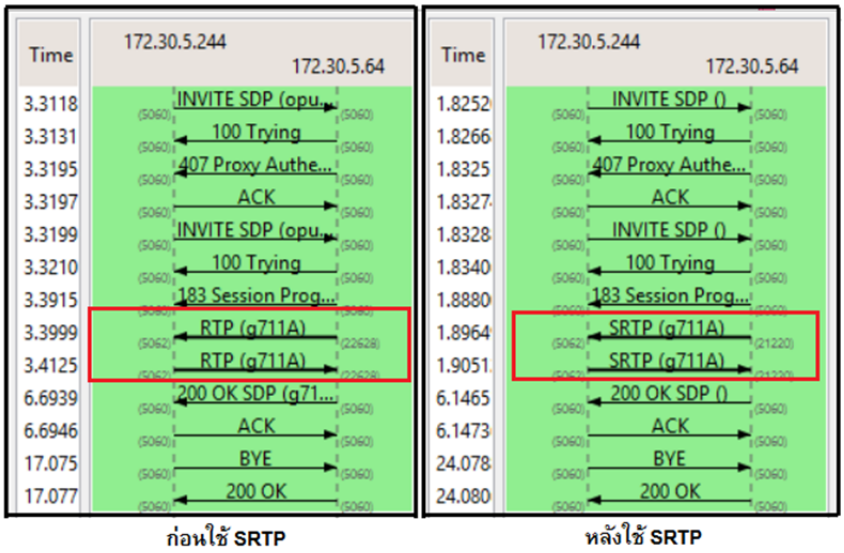
รูปที่ 4.2 ตัวอย่างการ Block หมายเลขไอพีต้นทางที่แสดงทาง Web User Interface

3) Cancel/Bye Attack

Cancel/Bye Attack โดยใช้ชุดคำสั่ง teardown ใน Kali Linux เพื่อทำการตัดสายโทรศัพท์ สิ้นสุดการสื่อสารของผู้ใช้งาน ผลปรากฏว่าไม่ส่งผลใดต่อระบบ ISANBox.F เนื่องจากช่องสัญญาณ SIP จะถูกเข้ารหัสป้องกันด้วย TLS ได้ ดังตัวอย่างการดักจับแล้วพบมีการเข้ารหัสสัญญาณในรูปที่ 4.1

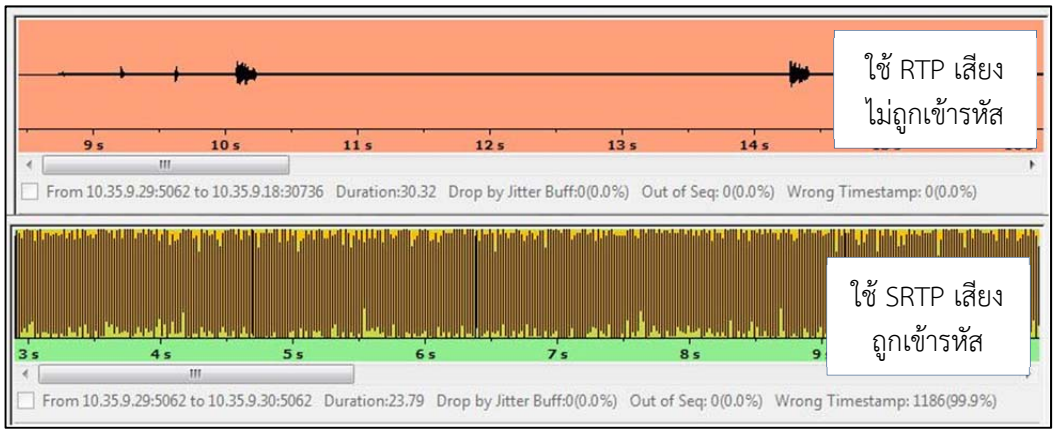
4) RTP Sniffing

RTP Sniffing ด้วยโปรแกรม Cain & Abel โดยโจมตีเพื่อดักจับ RTP Streaming แล้วฟังเสียงการสนทนา ปรากฏว่าระบบ ISANBox.F จะถูกดักจับข้อมูลเสียงได้ แต่เสียงที่ได้จะมีลักษณะที่มนุษย์ฟังไม่รู้เรื่องเนื่องจากถูกเข้ารหัส เมื่อใช้โปรแกรม Wireshark จับกราฟการไหลของแพ็กเก็ตจะได้ตัวอย่างแพ็กเก็ตดัง ดังในรูปที่ 4.3



รูปที่ 4.3 Flow of RTP/SRTP Packet

และมีลักษณะกราฟเสียงที่ถูกเข้ารหัสด้วยโพรโทคอล SRTP จากโปรแกรม Wireshark ดังแสดงตัวอย่างในรูปที่ 4.4



รูปที่ 4.4 ลักษณะเสียงที่ถูกเข้ารหัสและไม่เข้ารหัสจากโปรแกรม Wireshark

4.1.2 ผลการประเมินคุณภาพการให้บริการของระบบ ISANBox.F

จากการประเมินคุณภาพการให้บริการของ ISANBox.F และ FreeSWITCH รุ่น 1.2.6 ตามเทคนิควิธี E-Model ภายใต้ข้อจำกัดในเรื่องของ Bandwidth ที่ต่างกันซึ่งได้ผลคือมีค่า MOS อยู่ในระดับที่ดี นั่นหมายถึงผู้ใช้งานจะมีความพึงพอใจต่อคุณภาพเสียงที่ได้ยินคือมีลักษณะเสียงที่ดีใช้ได้ เสียงไม่ขาดหาย ผู้ใช้มีความรู้สึกพอใจกับคุณภาพเสียง และเป็นไปตามมาตรฐานที่ กสทช. กำหนดไว้ งแสดงรายละเอียดค่า MOS ในรูปที่ 2.5

ตารางที่ 4.1 คุณภาพการให้บริการของระบบ ISANBox.F และ FreeSWITCH 1.2.6 (MOS)

Bandwidth	**ค่าเฉลี่ย Mean Opinion Score (MOS)**				
	FreeSWITCH 1.2.6		**ISANBox.F**		**ค่า MOS**
	R-Factor	MOS	R-Factor	MOS	**ลดลง %**
3 Mbps	49.09 ± 1.24	2.52 ± 0.05 (1)	41.93 ± 1.2	2.15 ± 0.06 (1)	14.34
5 Mbps	59.52 ± 1.95	3.01 ± 0.09 (2)	54.98 ± 0.93	2.83 ± 0.05 (2)	5.98
10 Mbps	90.86 ± 1.07	4.31 ± 0.07 (6)	90.55 ± 1.17	4.27 ± 0.04 (5)	0.92
100 Mbps	91.93 ± 0.79	4.35 ± 0.02 (6)	90.72 ± 0.90	4.32 ± 0.07 (6)	0.68

(6) Very Satisfied > 4.3 (4) Some Users Dissatisfied 3.6 – 3.9 (2) Nearly All Users Dissatisfied 2.6 – 3.0

(5) Satisfied 4.0 - 4.29 (3) Many Users Dissatisfied 3.1 – 3.6 (1) Not Recommended 1 – 2.5

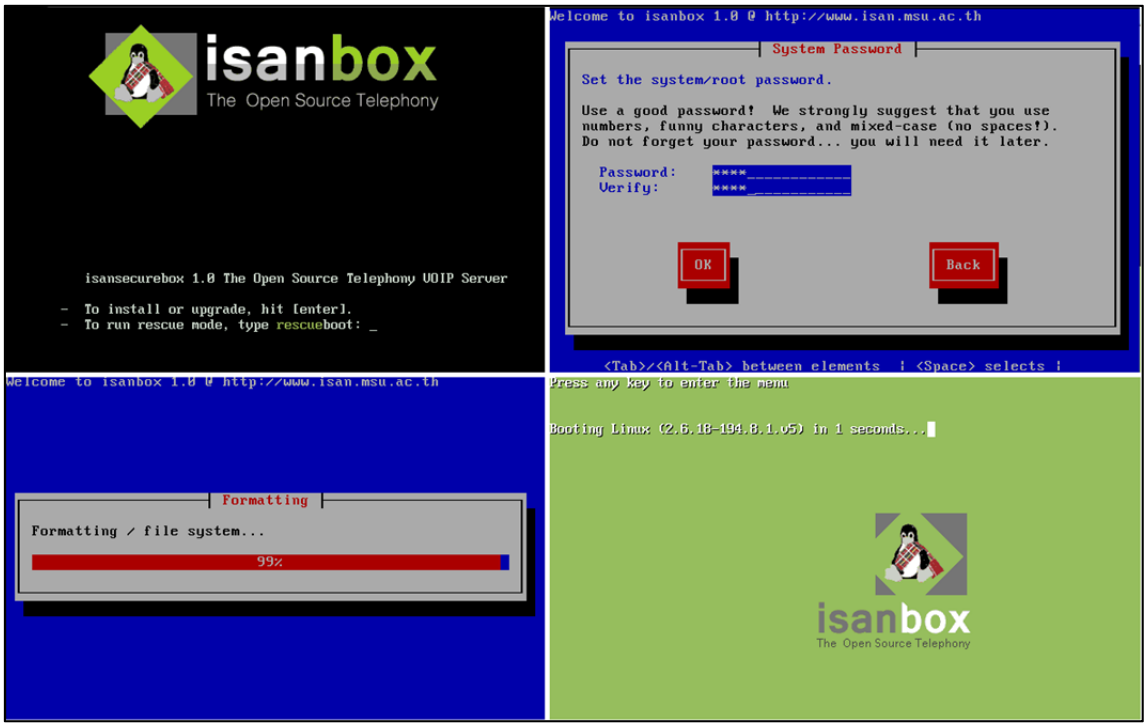
จากตารางที่ 4.1 ได้แสดงผลการทดลองเป็นค่าเฉลี่ย ($\bar{x}$) ของค่า MOS ที่ได้จากการวัดคุณภาพการให้บริการด้วยวิธี E Model ที่ช่วงความเชื่อมั่น 95 % ของ ISANBox.F ใน Bandwidth 3 Mbps ได้ค่า MOS 2.15 ± 0.06 Bandwidth 5 Mbps ได้ค่า MOS 2.83 ± 0.05 Bandwidth 10 Mbps ได้ค่า MOS 4.27 ± 0.04 และ Bandwidth 100 Mbps ได้ค่า MOS 4.32 ± 0.07

และค่า MOS ของ FreeSWITCH รุ่น 1.2.6 ใน Bandwidth 3 Mbps ได้ค่า MOS 2.52 ± 0.05 Bandwidth 5 Mbps ได้ค่า MOS 3.01 ± 0.09 Bandwidth 10 Mbps ได้ค่า MOS 4.31 ± 0.07 และ Bandwidth 100 Mbps ได้ค่า MOS 4.35 ± 0.02

จากการทดลองวัดคุณภาพการให้บริการพบว่า FreeSWITCH 1.2.6 จะมีค่า MOS มากกว่า ISANBox.F เพราะเป็นผลจากการเข้ารหัสจึงทำให้คุณภาพการให้บริการต่ำลง ซึ่งสอดคล้องกับงานวิจัย [12, 15, 26] และในสภาพ Bandwidth 100 Mbps ISANBox.F จะมีค่า MOS ลดลง 0.68 % ซึ่งมีค่ามากกว่า 4.3 นั่นหมายความว่ายังอยู่ในระดับผู้ใช้งานมีความพึงพอใจมาก และเมื่อทำการลดขนาดของ Bandwidth 10 Mbps พบว่าค่า MOS ลดลงมา 0.92 % นั่นหมายความคุณภาพการให้บริการลดลงมาอยู่ในระดับผู้ใช้งานมีความพึงพอใจ และในเมื่อลด Bandwidth ลงมาที่ 3 Mbps และ 5 Mbps พบว่าค่า MOS ของทั้ง 2 ก็ลดลงมาเรื่อยๆ ซึ่งต่ำกว่ากว่ามาตรฐานกำหนด ดังนั้นจากผลการทดลองจึงสรุปได้ในสภาพปกติ Bandwidth 100 Mbps คุณภาพการให้บริการของ ISANBox.F จะไม่ลดลง ใน Bandwidth 10 Mbps คุณการให้บริการจะลดลงจากระดับที่ผู้ใช้มีความพึงพอใจมากมาเป็นระดับผู้ใช้มีความพึงพอใจ และ Bandwidth 3 Mbps และ 5 Mbps ทั้งสองระบบมีคุณภาพการให้บริการต่ำกว่าที่มาตรฐานของ กสทช. กำหนดไว้คือค่า MOS น้อยกว่า 3.6 ซึ่งหากมีการนำเอาระบบ ISANBox.F ไปใช้งานในเครือข่ายระบบที่ใหญ่ขึ้นเช่น เครือข่าย MAN ก็จะไม่ส่งผลต่อคุณภาพการให้บริการมากนักเนื่องในเครือข่ายระดับ MAN ในปัจจุบันจะมี Bandwidth ที่เพียงพอต่อการใช้งาน ดังที่เห็นได้จากงานงานวิจัยของ สำเริง คำมีวงษ์ [45] ที่แสดงเห็นถึงคุณภาพการให้บริการของระบบ ISANBox.A รุ่นที่ 3.0 บนเครือข่ายระดับ MAN ที่มีการเพิ่มประสิทธิภาพด้านความมั่นคงซึ่งก่อให้เกิด Overhead ด้านคุณภาพเสียง ทดลองในเครือข่ายภายในของมหาวิทยาลัยราชภัฏร้อยเอ็ด โดยสภาพเครือข่ายไม่มีการแยก VLAN และ Physical network ของ VoIP กับ Data Traffic ออกจากกัน ผลการทดลองพบว่า หลังจากการเพิ่มประสิทธิภาพด้านความมั่นคงส่งผลให้มีผลค่าR-factor ลดลงเพียง 1.45 % คือจาก 92.75 ± 0.92 ไปเป็น 91.40 ± 1.74 จะเห็นว่าในเครือข่ายระดับ MAN ดังกล่าว โดยแม้จะมี Overhead เพิ่มขึ้นมาแต่คุณภาพการให้บริการหรือค่า MOS ก็ยังอยู่ในระดับที่ดีมากในทั้งก่อนและหลังการเพิ่มประสิทธิภาพด้านความมั่นคง

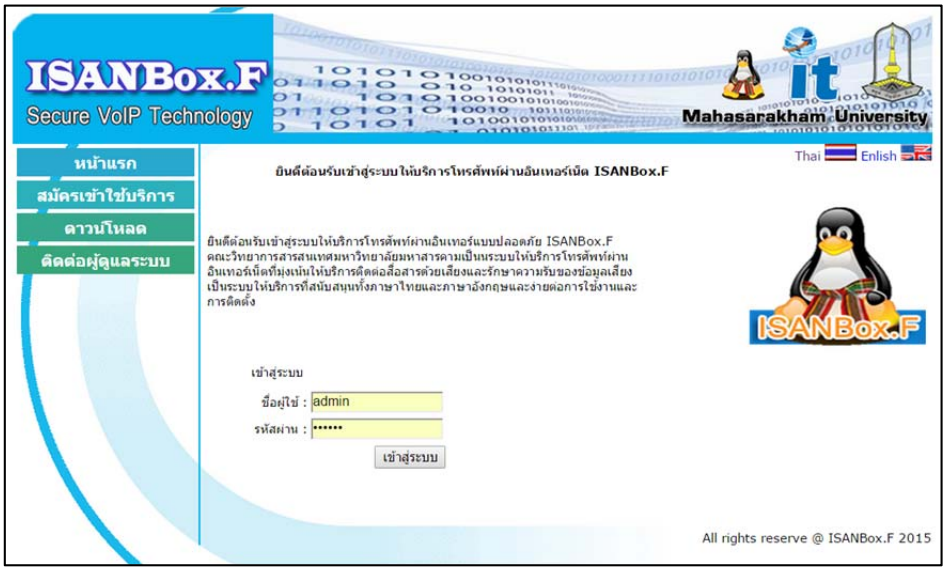
4.1.3 ผลการพัฒนาส่วนติดตั้งและส่วนติดต่อผู้ใช้งาน ISANBox.F

จากงานวิจัยทำให้ได้ระบบ VoIP ที่มีส่วน Web User Interface ที่ใช้งานง่าย อีกทั้งยังมีคุณสมบัติทางด้านความมั่นคง ได้ระบบที่มีคุณภาพการให้บริการเป็นไปตามมาตรฐานที่ กสทช. กำหนด ได้พัฒนาแผ่นติดตั้งแบบอัตโนมัติ สะดวกในการติดตั้งใช้งานพร้อมคู่มือที่ชัดเจน ดังแสดงตัวอย่างการติดตั้งในรูปที่ 4.5 และรายละเอียดดังในภาคผนวก ก



รูปที่ 4.5 ส่วนการติดตั้ง

งานวิจัยได้พัฒนา Web User Interface ที่มีความสะดวก ใช้งานง่ายสนับสนุนภาษาไทย สามารถจัดการ เพิ่ม ลบ แก้ไข ผู้ใช้งานระบบ VoIP ได้ผ่านทางหน้าเว็บดังแสดงตัวอย่าง Web User Interface ในรูปที่ 4.6 และมีวิธีใช้งานดังในภาคผนวก ข



รูปที่ 4.6 Web User Interface

4.1.4 ผลการประเมินเวลาในการใช้งานส่วนติดตั้งและส่วนติดต่อผู้ใช้งาน

การติดตั้งและใช้งานระบบ FreeSWITCH จากระบบเดิมที่ต้องใช้การป้อนคำสั่งเป็น Command line หรือการแก้ไขไฟล์คอนฟิก หรือที่เรียกว่า Text User Interface เพื่อตั้งค่าต่างๆ นั้น เป็นเรื่องที่ยุ่งยาก ซับซ้อน ต้องอาศัย ผู้ดูแลระบบที่มีความรู้ความสามารถเฉพาะด้านจึงจะติดตั้งและใช้งานระบบได้ และยังเป็นปัญหาสำหรับผู้ใช้งานทั่วไปที่ต้องการนำระบบ VoIP ไปใช้งาน ต่างจาก ISANBox.F ที่พัฒนาส่วนติดตั้งและส่วนติดต่อผู้ใช้งานขึ้นมา ซึ่งสามารถแก้ไขปัญหาดังกล่าวได้ ทำให้ผู้ใช้งานมีความสะดวก และง่ายต่อการใช้งาน ซึ่งจากการทดสอบวัดเวลาในการเข้าใช้งานในส่วนติดตั้งและส่วนติดต่อผู้ใช้งานใน FreeSWITCH แบบเดิม และใน ISANBox.F ด้วยวิธี KLM มีผลการทดสอบเวลาที่ใช้ในการทำกิจกรรมต่างๆ บนส่วนติดต่อผู้ใช้งานดังนี้

1) ส่วนติดตั้ง

วิทยานิพนธ์นี้ได้ทำการทดสอบวัดเวลาในการติดตั้ง FreeSWITCH โดยใช้วิธี KLM โดยจะทำการวัดเวลาตั้งแต่เริ่มติดตั้ง โดยจะไม่คิดเวลาที่ใช้ในการประมวลผลของขั้นตอนต่างๆ ซึ่งมีผลการทดสอบดังตารางที่ 4.2

ตารางที่ 4.2 ผลการประเมินเวลาการติดตั้ง FreeSWITCH

การกระทำ	รายละเอียด	เวลาที่ใช้ (วินาที)
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35
P	เลื่อนเมาส์ไปหน้าจอรับคำสั่ง Command	1.10
H	สลับจากเมาส์หรือแป้นพิมพ์	0.40
K	*พิมพ์ Command เพื่อติดตั้งแพ็กเก็ตที่จำเป็นต่อการติดตั้ง FreeSWITCH เช่น PHP, MySQL, Apache, และแพ็กเก็ต Development	52.8
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35
K	*พิมพ์ Command เพื่อแตกไฟล์ FreeSWITCH	16.6
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35
K	*พิมพ์ Command เพื่อ Compile FreeSWITCH	17.8
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35
K	*พิมพ์ Command เพื่อติดตั้ง Sound Module	8.4
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35
K	*พิมพ์ Command ย้ายตำแหน่งไปยังแฟ้มที่เก็บผู้ใช้งาน	9.6
K	พิมพ์คำสั่งสร้างโปรไฟล์ของผู้ใช้งาน	2.6
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35
K	พิมพ์โครงสร้างโปรไฟล์ของผู้ใช้	77.2
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35

ตารางที่ 4.2 ผลการประเมินเวลาการติดตั้ง FreeSWITCH (ต่อ)

การกระทำ	รายละเอียด	เวลาที่ใช้ (วินาที)
K	พิมพ์คำสั่งย้ายตำแหน่งไปยังแฟ้มของ FreeSWITCH	5.4
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35
K	*พิมพ์ Command เพื่อเปิด Service FreeSWITCH	2.6
K	พิมพ์ใน Command FreeSWITCH เพื่อตรวจความพร้อมใช้งานของ SIP Server	3.4
	รวม	208.7

*กรณีพิมพ์คำสั่ง Command คำนวณจาก จำนวนอักขระ x 0.20

จากตารางที่ 4.2 พบว่าการติดตั้งใช้งาน FreeSWITCH โดยการใช้ Command Line นั้น นับว่าเป็นวิธีที่ซับซ้อนและยุ่งยากพอสมควร โดยเฉพาะการต้องจดจำและพิมพ์คำสั่งจำนวนมากให้ถูกต้อง ดังจะเห็นได้จากผลการใช้เวลาในการพิมพ์คำสั่งต่างๆ ถึง 208.7 วินาที

จากนั้นได้ทำการทดสอบวัดเวลาในการติดตั้ง ISANBox.F โดยใช้วิธี KLM โดยจะทำการวัดเวลาตั้งแต่เริ่มติดตั้งจนถึงระบบพร้อมใช้งาน โดยจะไม่คิดเวลาที่ใช้ในการประมวลผลของขั้นตอนต่างๆ ซึ่งมีผลการทดสอบดังตารางที่ 4.3

ตารางที่ 4.3 ผลการประเมินเวลาการติดตั้ง ISANBox.F

การกระทำ	รายละเอียด	เวลาที่ใช้ (วินาที)
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35
K	กดปุ่ม Enter เพื่อเข้าสู่การติดตั้ง	0.20
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35
K	กดแป้นพิมพ์เลือกภาษา แล้ว กดปุ่ม OK เพื่อเลือกภาษา	0.8
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35
K	กดแป้นพิมพ์เลือกชนิดแป้นพิมพ์ แล้ว กดปุ่ม OK	0.4
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35
K	กดแป้นพิมพ์เลือกรูปแบบการติดตั้งกด แล้ว กดปุ่ม OK	0.40
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35
K	กดแป้นพิมพ์เลือกรูป IP แล้วกดปุ่ม OK	0.4
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35
K	กดแป้นพิมพ์หมายเลข IP Server แล้ว กดปุ่ม OK	3.8

ตารางที่ 4.3 ผลการประเมินเวลาการติดตั้ง ISANBox.F (ต่อ)

การกระทำ	รายละเอียด	เวลาที่ใช้ (วินาที)
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35
K	กดแป้นพิมพ์เพื่อตั้งรหัสผ่าน แล้วกดปุ่ม OK	2.8
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35
K	กดปุ่ม Reboot เพื่อเริ่มต้นระบบ ISANBox.F	0.4
	รวม	18.65

*กรณีกดแป้นพิมพ์เพื่อทำกิจกรรมบางอย่างคำนวณจาก จำนวนอักขระ x 0.20

จากตารางที่ 4.3 เป็นขั้นตอนการติดตั้ง ISANBox.F ซึ่งเป็นการใช้แป้นพิมพ์ในการเลือกและป้อนคำสั่งเพียงอย่างเดียวก็สามารถติดตั้งระบบได้อย่างสะดวกและรวดเร็ว เมื่อคำนวณเวลาในการติดตั้งโดยไม่คิดรวมเวลาที่ใช้ในการประมวลผลของขั้นตอนต่างๆพบว่ามีการใช้เวลาเพียง 18.65 วินาที

จะเห็นได้ว่าส่วนติดตั้งของระบบ ISANBox.F จะใช้เวลาในการติดตั้งตั้งน้อยกว่าการติดตั้ง FreeSWITCH ในแบบเดิมหลายเท่าตัว อีกทั้งการติดตั้งระบบ VoIP โดยการใช้ระบบ ISANBox.F ยังทำให้ผู้ใช้โดยทั่วไปที่ไม่จำเป็นต้องมีความรู้ทางด้านเครือข่ายในระดับสูง ก็สามารถติดตั้งระบบ VoIP และใช้งานได้อย่างสะดวก อีกทั้งระบบ ISANBox.F ยังมีคู่มือการติดตั้งใช้งานที่เป็นภาษาไทยให้ผู้ใช้อีกด้วย

2) ส่วนติดต่อผู้ใช้งาน

วิทยานิพนธ์นี้ได้ทำการทดสอบวัดเวลาในการใช้งาน FreeSWITCH โดยใช้วิธี KLM โดยจะทำการวัดเวลา การเปิดปิดฟังก์ชันการเข้ารหัสเสียง โดยจะไม่คิดเวลาที่ใช้ในการประมวลผลของขั้นตอนต่างๆ ซึ่งมีผลการทดสอบดังตารางที่ 4.4

ตารางที่ 4.4 ผลการประเมินเวลาการ เปิด/ปิด SRTP ใน FreeSWITCH

การกระทำ	รายละเอียด	เวลาที่ใช้ (วินาที)
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35
K	พิมพ์คำสั่งย้ายตำแหน่งไปยังแฟ้มของ FreeSWITCH	9.6
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35
K	พิมพ์คำสั่งเปิดไฟล์คอนฟิกเพื่อแก้ไขค่าพารามิเตอร์	3.2
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35
K	กดแป้นพิมพ์เลื่อนตัวชี้ตำแหน่งไปยังแท็กที่ต้องการแก้ไข	9
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35

ตารางที่ 4.4 ผลการประเมินเวลาการ เปิด/ปิด SRTP ใน FreeSWITCH (ต่อ)

การกระทำ	รายละเอียด	เวลาที่ใช้ (วินาที)
K	พิมพ์แก้ไขค่าพารามิเตอร์ในการเข้ารหัสแล้วบันทึก	2.8
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35
K	พิมพ์คำสั่งย้ายตำแหน่งไปยังแฟ้มของ FreeSWITCH	9.6
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35
K	พิมพ์คำสั่ง SIP Reload เพื่อเริ่มต้นค่าคอนฟิกใหม่	2.2
	รวม	44.5

*กรณีพิมพ์คำสั่ง Command คำนวณจาก จำนวนอักขระ x 0.20

จากตารางที่ 4.4 พบว่าเวลารวมในการทำงานเปิดใช้งานฟังก์ชั่นเข้ารหัสเสียงใช้เวลาถึง 44.5 วินาที ซึ่งเป็นเวลาที่ค่อนข้างมากเนื่องจากเป็นการทำงานผ่าน Text User Interface โดยการป้อนคำสั่งด้วยการพิมพ์บนแป้นพิมพ์เพียงอย่างเดียว

จากนั้นได้ทำการทดสอบวัดเวลาในใช้งานผ่านส่วนติดต่อผู้ใช้งานของ ISANBox.F ด้วยการเปิดใช้งานฟังก์ชันเข้ารหัส แล้ววัดเวลาการใช้งานด้วยวิธี KLM โดยจะไม่คิดเวลาที่ใช้ในการประมวลผลของขั้นตอนต่างๆ ซึ่งมีผลการทดสอบตารางที่ 4.5

ตารางที่ 4.5 ผลการประเมินเวลาการ เปิด/ปิด SRTP ใน ISANBox.F

การกระทำ	รายละเอียด	เวลาที่ใช้ (วินาที)
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35
P	เลื่อนเม้าส์ไปชี้เมนูเปิด/ปิด SRTP	1.10
P	กดเมาส์เลือกเมนู	0.20
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35
P	เลื่อนเมาส์ไปฟังก์ชัน เปิด/ปิด SRTP	1.10
P	กดเมาส์เลือกเมนูเลือกฟังก์ชัน	0.20
M	การใช้ความคิดทำกิจกรรมบางอย่าง	1.35
P	เลื่อนเมาส์ไปปุ่มบันทึก	1.10
P	กดปุ่มบันทึก	0.20
	รวม	7.9

จากตารางที่ 4.5 พบว่าเวลารวมในการทำงานเปิดใช้งานฟังก์ชั่นเข้ารหัสเสียงใน ISANBox.F ใช้เวลาในการทำงานเพียง 7.9 วินาที สืบเนื่องจากใน ISANBox.F ผ่าน Web User Intreface จึงทำให้ผู้ใช้เกิดความสะดวกและลดเวลาในการทำงานลงเมื่อเทียบกับการใช้ในงาน FreeSWITCH แบบเดิม

4.1.5 เปรียบเทียบคุณสมบัติ ISANBox.F กับ Bluebox

สืบเนื่องจากซอฟต์แวร์ FreeSWITCH มีการพัฒนาเปลี่ยนผ่านรุ่นอยู่เป็นระยะ ซึ่งในปัจจุบัน (มิถุนายน พ.ศ. 2558) FreeSWITCH ได้มีการสนับสนุนให้ใช้ส่วนติดต่อผู้ใช้งาน (Graphic User Interface) ซึ่งพัฒนาให้ผู้ใช้ใช้งานได้อย่างสะดวกสบายในชื่อ Blue Box Project มีการพัฒนามาจนถึง BlueBox รุ่น 1.0.3 ด้วยเหตุนี้งานวิจัยก็ได้ทดลองติดตั้งใช้งานตามค่าเริ่มต้นของระบบศึกษาการทำงานและฟังก์ชันต่างๆ ของ BlueBox จึงได้ทำการเปรียบเทียบถึงคุณสมบัติระหว่าง ISANBox.F กับ BlueBox ได้ผลดังแสดงในตารางที่ 4.6

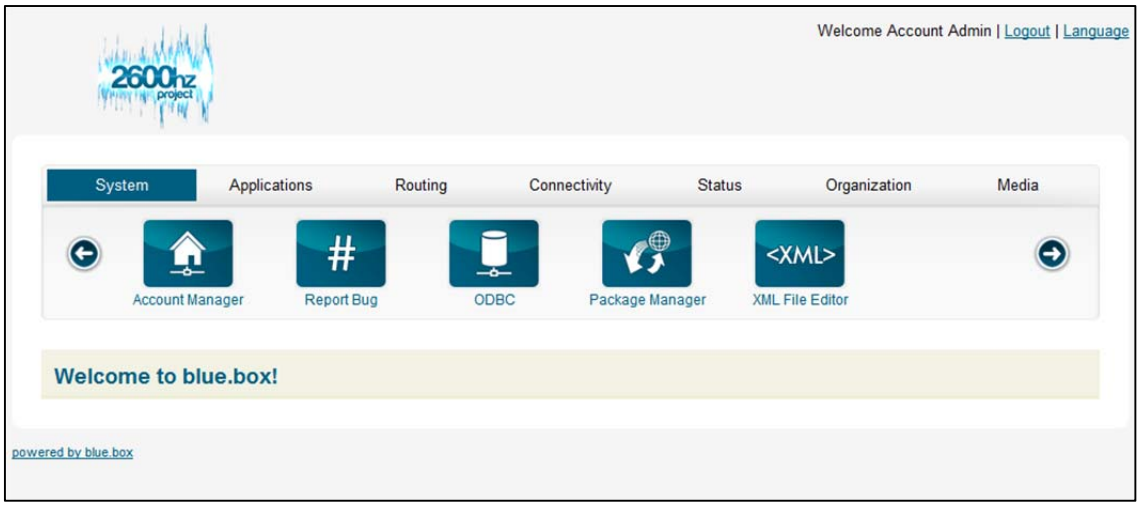
ตารางที่ 4.6 เปรียบเทียบคุณสมบัติของ ISANBox.F และ BlueBox

Feature	ISANBox.F	BlueBox
Installation Module	/	/
Web Graphic User Interface	/	/
Cancel/Bye Attack Protected	/	x
SIP Flooding Protected	/	x
SIP Register Hijacking Protected	/	x
RTP Sniffing Protected	/	x

/: Support x: Not Support

จากตารางที่ 4.6 พบว่าคุณสมบัติหลักๆ ที่ BlueBox ได้พัฒนาคือมุ่งเน้นที่ความสะดวกสบาย สวยงาม และส่วนติดตั้งใช้งานง่าย ส่วนด้านความมั่นคงก็ยังไม่ป้องกันการโจมตีในแบบ SIP Flooding และการโจมตีแบบอื่นๆ ก็ยังป้องกันไม่ได้เนื่องจากยังไม่มีการแนะนำและเปิดใช้งานฟังก์ชันด้านความมั่นคงที่ชัดเจนซึ่ง BlueBox ไม่ได้ถูกพัฒนามาเพื่อแก้ปัญหาด้านความมั่นคง

ซึ่งต่างจาก ISANBox.F ที่วิทยานิพนธ์นี้ได้เสนอการพัฒนาเพื่อเพิ่มประสิทธิภาพทางด้านความมั่นคงของระบบเป็นหลักและยังมีส่วนของ User Interface และส่วนการติดตั้งที่ใช้งานง่ายอีกด้วย ดังแสดงภาพ User Interface ของ ISANBox.F ดังในรูปที่ 4.6 และตัวอย่าง User Interface ของ BlueBox ดังในรูปที่ 4.7



รูปที่ 4.7 Web User Interface of Bluebox

จากการพัฒนาระบบ ISANBox.F ทำให้ได้ระบบที่มีความสามารถในการป้องกันการโจมตี SIP Register Hijacking ป้องกันการโจมตี Cancel/Bye Attack แก้ไขปัญหาการดักฟังเสียงการสนทนา (RTP Sniffing) และป้องกันการจู่โจมแบบ SIP Flooding ซึ่งจะทำให้เกิดผลดีกับองค์กรในด้านการรักษาความลับของข้อมูลเสียงและความมั่นคงของระบบ ISANBox.F ยังเป็นระบบที่มีคุณภาพการให้บริการในระดับที่ดีกว่ามาตรฐานกำหนด ผู้ใช้งานพึงพอใจ มีระบบที่ติดตั้งและใช้งานง่ายรวดเร็ว มี Web User Interface ที่สนับสนุนภาษาไทย อีกทั้งยังเป็นผลดีกับเศรษฐกิจองค์รวมของประเทศเพราะไม่ต้องพึ่งพาซอฟต์แวร์ราคาแพงจากต่างประเทศ ทำให้การสื่อสารด้วย VoIP ไม่จำกัดอยู่แคในองค์กรที่มีขนาดใหญ่และมีงบประมาณในการลงทุนสูงอีกต่อไป

เนื่องจากซอฟต์แวร์ FreeSWITCH มีการพัฒนาเปลี่ยนผ่านรุ่น อย่างรวดเร็ว ซึ่งในขณะที่วิทยานิพนธ์นี้ได้ศึกษาทดลองอยู่นั้นได้เลือกใช้รุ่น 1.2.6 เนื่องจากเป็นรุ่นที่มีความเสถียรและคงที่ในขณะนั้น ดังนั้นจึงเลือกใช้รุ่น 1.2.6 ในการเป็นฐานพัฒนาต่อยอด แต่ในขณะกำลังเขียนวิทยานิพนธ์ฉบับนี้ (มิถุนายน พ.ศ. 2558) มีรุ่น 1.4.19 ออกมาล่าสุด งานวิจัยจึงได้ทดสอบประสิทธิภาพทางด้านความมั่นคงตาม ซึ่งผลการทดลองเห็นได้ว่า FreeSWITCH รุ่น 1.4.19 ยังคงมีปัญหาด้านความมั่นคงไม่ต่างจากรุ่น 1.2.6 ที่ใช้ในวิทยานิพนธ์นี้

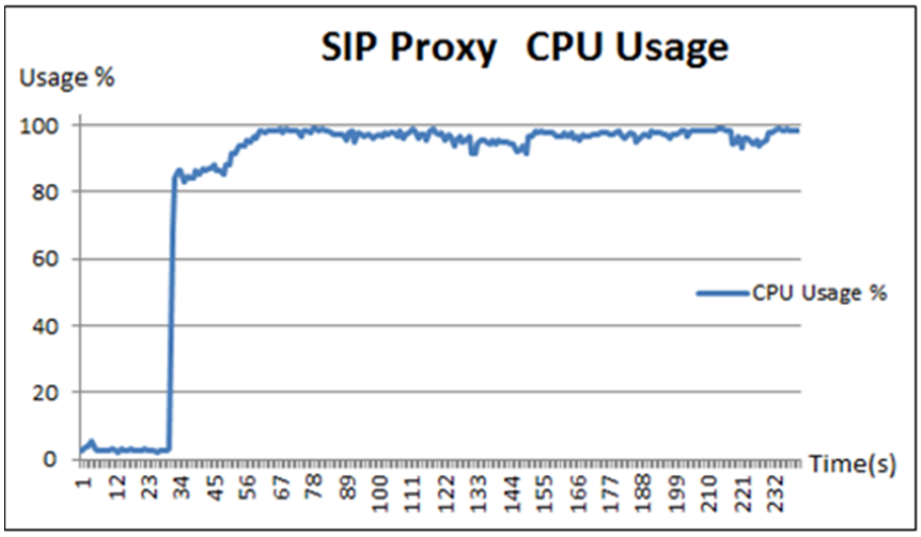
4.2 ผลการออกแบบแนวทางแก้ไขปัญหา SIP Flooding

วิทยานิพนธ์นี้ได้ทำการทดลองตามแนวทางแก้ไขปัญหา SIP Flooding ที่ได้เสนอไว้ในบทที่ 3 และได้ทดสอบประสิทธิภาพของต้นแบบแนวทางแก้ไขปัญหาซึ่งมีราละเอียดดังนี้

4.2.1 ผลการทดสอบประสิทธิภาพของ SIP Proxy ที่ถูกโจมตีด้วยเทคนิค SIP Flooding

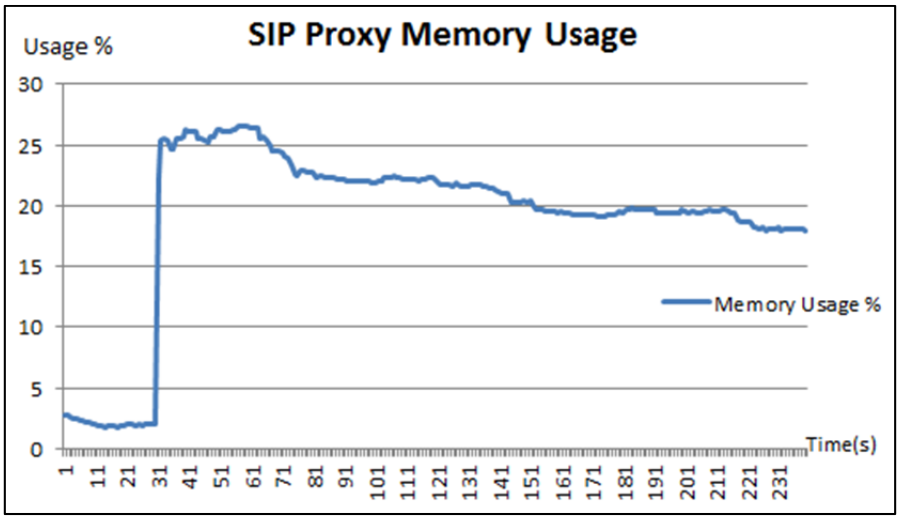
เมื่อทดลองส่งข้อความ Invite Flood มายัง SIP Proxy ที่ไม่มีการป้องกันการโจมตี ดังกล่าวปรากฏว่าช่วง 30 วินาทีแรกก่อนการโจมตี CPU มีการทำงาน 2.97 ± 0.22 % เมื่อเข้าสู่

ช่วงเวลาการโจมตี 60 วินาทีก็พบว่า CPU มีภาระการทำงานขึ้น 93.16 ± 1.61 % หลังจากการโจมตี 120 วินาที พบว่ามีการใช้งาน CPU 96.66 ± 0.55 % และ หลังจากนั้นอีก 30 วินาที พบว่า CPU มีการทำงาน 97.06 ± 0.65 % ซึ่งก็ยังไม่กลับเข้าสู่สภาวะปกติของระบบ ระบบไม่สามารถให้บริการผู้ใช้อื่นได้เป็นเวลานานแล้วเกิดการไม่ตอบสนองในที่สุด ดังแสดงตัวอย่างการทำงานของ CPU ในรูปที่ 4.8



รูปที่ 4.8 การทำงานของ CPU เมื่อถูกโจมตีด้วย SIP Flooding

ผลการทดลองโจมตี SIP Flooding สงผลให้ระบบมีใช้งาน Memory ในขณะก่อนการโจมตี 30 วินาที 2.06 ± 010 % ขณะการโจมตี 60 วินาที ใช้งาน Memory 24.67 ± 0.39 % หลังการโจมตี 120 วินาที มีการใช้ Memory 20.64 ± 0.04 % หลังจากนั้นอีก 30 วินาที พบว่ามีการใช้งาน Memory 1.96 ± 0.21 % ซึ่งเป็นการกลับเข้าสู่สภาวะปกติของระบบ ดังแสดงตัวอย่างการใช้ Memory รูปที่ 4.9



รูปที่ 4.9 การทำงานของ Memory เมื่อถูกโจมตีด้วย SIP Flooding

จากผลการทดลอง ผลการใช้งาน CPU และ Memory ของระบบในแต่ละช่วงเวลาในการทดลองนั้นพบว่า CPU จะได้รับผลกระทบคือมีภาระงานมากขึ้นอย่างเห็นได้ชัด และการทำงานของ Memory ของระบบ จะเพิ่มขึ้นตามไปด้วยจนทำให้ระบบไม่ตอบสนองในที่สุด แต่การฟื้นตัวของ Memory จะช้ากว่า CPU เนื่องจากเหตุผลทางด้านสถาปัตยกรรมคอมพิวเตอร์ที่ Memory จะต้องถือครองทรัพยากรของระบบแล้วค่อยๆปล่อยให้กลับสู่สภาพปกติตามหลังกระบวนการฟื้นตัวของ CPU ดังจะเห็นได้จากแนวโน้มการฟื้นตัวของ CPU และ Memory แสดงการใช้งานทรัพยากรในตารางที่ 4.7

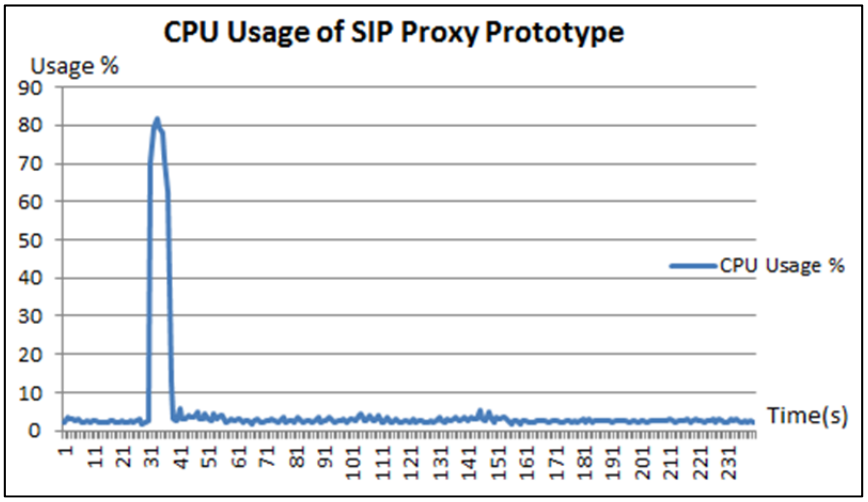
ตารางที่ 4.7 การใช้งาน CPU และ Memory ก่อนป้องกัน SIP Flooding

Resource Usage	Before 30	Attack 60	After 120	After 30
CPU Usage (%)	2.97 ± 0.22	93.16 1.61	96.66 ± 0.55	97.06 ± 0.65
Memory Usage (%)	2.06 ± 010	24.67 ± 0.39	20.64 ± 0.04	1.96 ± 0.21

และที่สำคัญในขณะที่ SIP Proxy ถูกโจมตี SIP Client อื่นจะไม่สามารถร้องข้อการสร้างเซสชั่นในการติดต่อสื่อสารได้ ซึ่งเป็นการเกิดการปฏิเสธการให้บริการจาก SIP Proxy

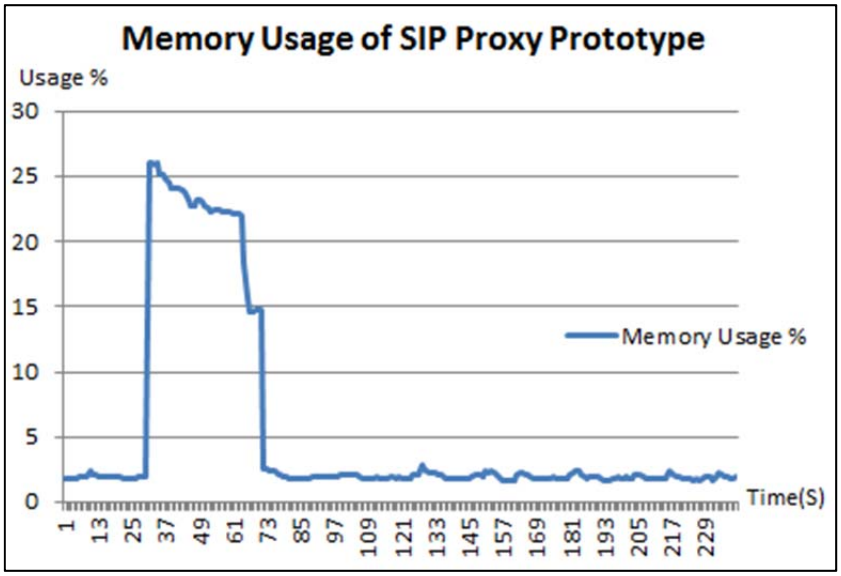
4.2.2 ผลการทดสอบประสิทธิภาพการป้องกัน SIP Flooding ของ SIP Proxy ต้นแบบ

เมื่อทดลองส่งข้อความ Invite Flood มายัง SIP Proxy ที่มีการป้องกันการโจมตีด้วยการวิเคราะห์ Response Message ปรากฏว่าช่วง 30 วินาทีแรกก่อนการโจมตี การทำงานของ CPU ยังอยู่ในสภาวะปกติคือ CPU มีการทำงาน 3.00 ± 0.62 % และเมื่อเข้าสู่ช่วงเวลาการโจมตี 60 วินาทีก็พบว่า CPU มีภาระการทำงานขึ้น 59.41 ± 0.20 % หลังจากการโจมตี 120 วินาที พบว่ามีการใช้งาน CPU 6.32 ± 2.72 % และ หลังจากนั้นอีก 30 วินาที พบว่า CPU มีการทำงาน 1.81 ± 0.05 % ซึ่งเป็นการกลับเข้าสู่สภาวะปกติของระบบ ดังแสดงตัวอย่างการทำงานของ CPU ในรูปที่ 4.10



รูปที่ 4.10 การทำงานของ CPU หลังจากที่ถูกป้องกัน SIP Flooding

ผลการทดลองโจมตี SIP Flooding สงผลให้ระบบมีใช้งาน Memory ในขณะก่อนการโจมตี 30 วินาที 1.93± 0.05 % ขณะการโจมตี 60 วินาที ใช้งาน Memory 17.75 ± 2.48 % หลังการโจมตี 120 วินาที มีการใช้ Memory 1.98 ± 0.04 % หลังจากนั้นอีก 30 วินาที พบว่ามีการใช้งาน Memory 1.80 ± 0.07 % ซึ่งเป็นการกลับเข้าสู่สภาวะปกติของระบบ ดังแสดงตัวอย่างการใช้ Memory รูปที่ 4.11



รูปที่ 4.11 การทำงานของ Memory หลังจากที่ถูกป้องกัน SIP Flooding

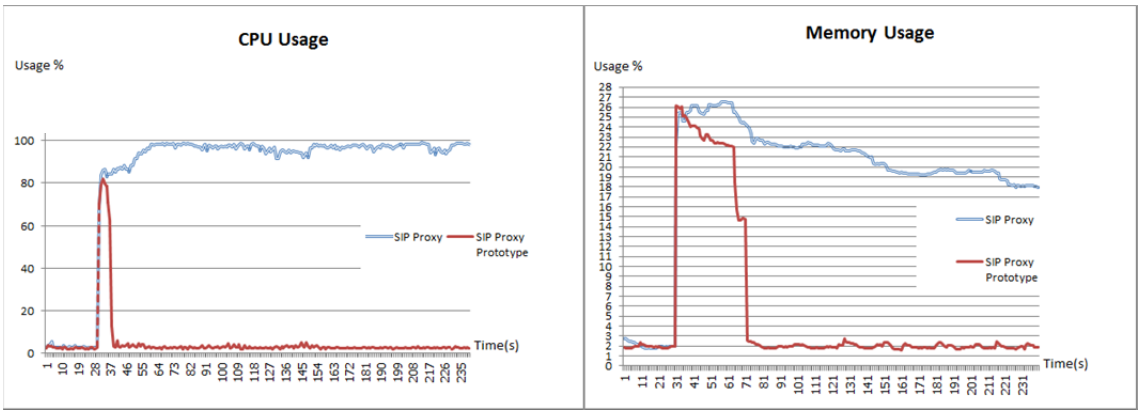
และที่สำคัญในขณะที่ SIP Proxy ถูกโจมตี SIP Client อื่นจะยังสามารถร้องข้อการสร้างเซสชั่นในการติดต่อสื่อสารได้ตามปกติและเมื่อมีการโจมตีด้วยในแบบเดิมจากต้นทางเดิมเข้ามาอีกครั้งก็จะไม่ส่งผลใดกับ SIP Proxy เนื่องจากระบบได้ทำการ Block หมาเลขไอพีต้นทางนั้นไปแล้ว แต่การฟื้นตัวของ Memory จะช้ากว่า CPU เนื่องจากเหตุผลทางด้านสถาปัตยกรรมคอมพิวเตอร์ที่ Memory จะถือครองทรัพยากรของระบบแล้วค่อยๆ ปล่อยให้กลับสู่สภาพปกติตามหลังกระบวนการฟื้นตัวของ CPU

จากผลการทดลอง ผลการใช้งาน CPU และ Memory ของระบบในแต่ละช่วงเวลาในการทดลองนั้นพบว่า CPU จะได้รับผลกระทบคือมีภาระงานมากเฉพาะในช่วงแรกที่มีการโจมตีซึ่งเกิดขึ้นในระยะสั้นๆ ทำให้ผู้ใช้ทั่วไปต้องรอการเชื่อมต่อเป็นเวลาสั้นๆ แต่การทำงานของ Memory ของระบบ จะเพิ่มขึ้นตามไปด้วยแต่ก็จะกลับเข้าสู่สภาวะปกติในเวลาต่อมา ดังแสดงการใช้งานทรัพยากรของระบบในตารางที่ 4.8

ตารางที่ 4.8 การใช้งาน CPU และ Memory หลังจากที่ถูกป้องกัน SIP Flooding

Resource Usage	Before 30	Attack 60	After 120	After 30
CPU Usage (%)	2.47 ± 0.14	93.16 ± 1.61	2.70 ± 0.20	2.57 ± 0.09
Memory Usage (%)	1.93± 0.05	17.75 ± 2.48	1.98 ± 0.04	1.80 ± 0.07

จากผลการทดลองจะสรุปได้ว่าการโจมตีด้วยเทคนิควิธี SIP Flooding นั้นส่งผลต่อการทำงานของ SIP Proxy คือจะทำให้มีภาระงานมากขึ้น มีการใช้งาน CPU และ Memory ของระบบมากกว่าปกติจนทำให้กระบวนการทำงานของ SIP Proxy ไม่สามารถให้บริการผู้ใช้โดยทั่วไปได้ ซึ่งใน SIP Proxy ต้นแบบที่มีการป้องกันโจมตีดังกล่าว พบว่าในครั้งแรกของการโจมตีทั้ง CPU และ Memory ก็จะมีภาระงานสูงขึ้นในช่วงแรกเท่านั้น เนื่องจากเป็นกระบวนการช่วง 10 แพ็กเก็ตแรกที่มีการตรวจวิเคราะห์พฤติกรรมเมื่อพบว่าเป็นการโจมตีก็จะส่งต่อให้ Iptables ทำการบล็อกหมายเลขไอพีนั้นทันที ในช่วงเวลากระบวนการนี้เองที่ยังมีแพ็กเก็ต Flood เข้ามายัง Proxy อยู่อย่างต่อเนื่อง และเนื่องจากมีอัตราการส่งแพ็กเก็ตที่เร็วกว่าปกติมากจึงทำให้ช่วงเวลาแรกยังมีแพ็กเก็ตเข้ามาทำให้ CPU และ Memory มีภาระงานที่สูงขึ้นแต่ก็เป็นเพียงช่วงเวลาสั้นๆ โดยหลังจากที่ Iptables ทำงาน CPU และ Memory ก็จะเริ่มกลับเข้าสู่สภาวะปกติ แต่เมื่อมีการโจมตีจากต้นทางเดิมในครั้งต่อไปก็จะไม่ส่งผลกระทบต่อระบบเนื่องจาก Iptables ได้บล็อกหมายเลขไอพีต้นทางเรียบร้อยแล้ว ดังแสดงตัวอย่างเปรียบเทียบการใช้งานของ CPU และ Memory ของระบบในรูปที่ 4.12



รูปที่ 4.12 เปรียบเทียบการใช้งานของ CPU และ Memory

จากรูปที่ 4.12 เห็นได้ชัดว่าการทำงานทำงานของ CPU และ Memory ของ SIP Proxy ต้นแบบที่มีการป้องกันการโจมตีนั้นจะมีภาระงานที่สูงขึ้นแต่เพียงระยะแรกเท่านั้น ก่อนจะค่อยๆ กลับคืนสู่สภาวะปกติ ซึ่งต่างจากกรณีที่ไม่มีการป้องกันการโจมตี จะมีการทำงานของ CPU และ Memory สูงกว่าปกติและจะใช้เวลาในการกลับสู่สภาวะปกตินานกว่าในการกรณีที่มีการป้องกัน SIP Flooding

ผลการทดสอบเวลาในการตอบสนองต่อการโจมตีของ SIP Proxy ต้นแบบ ซึ่งจากการทดลองพบว่า SIP Proxy ต้นแบบใช้เวลาในการตอบสนองเพียง 3.83 ± 0.12 มิลลิวินาที ซึ่งเมื่อเปรียบเทียบกับการตอบสนองการโจมตีของด้วยการอ่านไฟล์ Log ตามหัวข้อที่ 3.3.1 จะได้ผลดังตารางที่ 4.9

ตารางที่ 4.9 เปรียบเทียบเวลาที่ใช้ตอบสนองการโจมตีระหว่างการแก้ปัญหาด้วยการอ่านไฟล์ Log กับการแก้ปัญหาที่โพรโทคอล SIP

วิธีแก้ปัญหา SIP Flooding	เวลาการตอบสนองการโจมตี
การอ่านไฟล์ Log กรณีที่เร็วที่สุด	9.11 ± 0.10 วินาที
การอ่านไฟล์ Log กรณีที่ช้าที่สุด	38.09 ± 0.13 วินาที
การวิเคราะห์ข้อความ Response ที่โพรโทคอล SIP	3.83 ± 0.12 มิลลิวินาที

จากตารางที่ 4.9 จะได้ชัดว่าถึงแม้ในกรณีที่ตอบสนองเร็วที่สุดของการอ่านไฟล์ Log ก็ยังช้ากว่า วิธีการการวิเคราะห์ข้อความ Response ที่โพรโทคอล SIP ที่ใช้เวลาเพียง 3.83 ± 0.12 มิลลิวินาที ซึ่งเมื่อเทียบระหว่าง 2 วิธีดังกล่าวแล้วพบว่า วิธีการการวิเคราะห์ข้อความ Response ตามที่เสนอในวิทยานิพนธ์นี้จะใช้เวลาในการตอบสนองการโจมตีได้เร็วกว่าวิธีการอ่านไฟล์ Log ในกรณีที่เร็วที่สุดถึง 99.95 % ซึ่งการตอบสนองในกรณีที่เร็วที่สุดใช้เวลา 9.11 ± 0.10 วินาที โดยจะไม่ส่งผลกับ Proxy มากนัก แต่เมื่อพิจารณาถึงกรณีที่ช้าที่สุดของการอ่านไฟล์ Log ก็พบว่าใช้เวลานานถึง 38.09 ± 0.13 วินาที ซึ่งเวลาที่ใช้ในการตอบสนองของในกรณีที่ช้าที่สุดนี้ เป็นเวลาที่มากเพียงพอที่ทำจะให้ SIP Proxy เกิดการปฏิเสธการให้บริการต่อผู้ใช้ทั่วไป ทำให้ SIP Proxy ไม่ตอบสนอง และทำให้ระบบล้มเหลวลงในที่สุด

จะเห็นได้ว่าการที่แก้ปัญหา SIP Flooding ด้วยวิธีอ่านไฟล์ Log นั้น จะแก้ปัญหา SIP Flooding ได้อย่างมีประสิทธิภาพในกรณีที่การโจมตีนั้นเกิดขึ้นก่อนที่ Script ตรวจจับจะทำงาน (กรณีที่เร็วที่สุด) เท่านั้น แต่ก็มีความเป็นไปได้สูงในกรณีที่การโจมตีเกิดขึ้นหลังจากที่ Script ตรวจจับเพิ่งทำงานผ่านไป ทำให้มีโอกาสที่จะถูกโจมตีเป็นผลสำเร็จโดยที่การตรวจจับไม่สามารถตอบสนองทันต่อการโจมตี ซึ่งก็จะทำให้ระบบ VoIP ที่ใช้วิธีอ่านไฟล์ Log ในการแก้ไขปัญหาเกิดความเสียหาย ยิ่งถ้าหากเป็นระบบที่มีความเข้มงวดในการสื่อสาร เรื่องธุรกิจหรือการเงิน ก็จะยิ่งมีมูลค่าความเสียหายที่สูง

ดังนั้นการนำต้นแบบการป้องกันการโจมตี SIP Flooding โดยการวิเคราะห์ข้อความ Response ตามที่เสนอในวิทยานิพนธ์นี้ไปประยุกต์ใช้งานกับระบบ VoIP จะส่งผลดีต่อระบบการป้องกันในด้านประสิทธิภาพในการตอบสนองการโจมตีได้อย่างรวดเร็วและทันต่อเหตุการณ์ ลดโอกาสในการเกิดการปฏิเสธการให้บริการ และเสริมความมั่นคงให้กับระบบ VoIP ที่นำไปประยุกต์ใช้งานอีกด้วย

4.2.3 ผลการออกรายงานการโจมตีที่ไฟล์ Log และการแจ้งเตือนในกลุ่มผู้ดูแลระบบบน Facebook

วิทยานิพนธ์นี้ได้เสนอให้มีการออกรายงานการโจมตีในไฟล์ Log ของระบบ โดยมีรายละเอียดของการโจมตีประกอบไปด้วย วันที่ เวลา และหมายเลขไอพีต้นทางของการโจมตี เพื่อให้ผู้ดูแลระบบได้ตรวจสอบรายละเอียดการโจมตีอีกครั้ง ดังตัวอย่างไฟล์ Log ดังตัวอย่างการโจมตีในรูปที่ 4.13

```
1 23/05/2015 23:03:18 SIP Flooding From Source IP : 172.30.5.174
2 23/05/2015 23:06:47 SIP Flooding From Source IP : 172.30.5.174
3 23/05/2015 23:18:12 SIP Flooding From Source IP : 172.30.5.29
4 23/05/2015 23:19:34 SIP Flooding From Source IP : 172.30.5.29
5 25/05/2015 10:32:57 SIP Flooding From Source IP : 172.30.5.29
6 25/05/2015 10:40:27 SIP Flooding From Source IP : 172.30.5.29
7 25/05/2015 10:44:42 SIP Flooding From Source IP : 172.30.5.29
8 25/05/2015 10:50:10 SIP Flooding From Source IP : 172.30.5.29
9 25/05/2015 12:02:47 SIP Flooding From Source IP : 172.30.5.29
```

รูปที่ 4.13 ตัวอย่างไฟล์ Log การโจมตี

นอกจากมีการออกรายงานในรูปแบบไฟล์ Log แล้ว การออกแบบแนวคิดแก้ไขปัญหา SIP Flooding ยังเสนอให้มีระบบแจ้งเตือนการโจมตีผ่านทางเครือข่ายสังคมออนไลน์หรือกลุ่ม Facebook ของ VoIP Administrator Team (VAT) ดังแสดงตัสอย่างในรูปที่ 4.14

รูปที่ 4.14 การแจ้งเตือนการโจมตีในกลุ่มของ VoIP Administrator Team (VAT)

รูปที่ 4.14 แสดงถึงตัวอย่างการแจ้งเตือนการโจมตีโดยเมื่อระบบตรวจพบการโจมตีจะทำการโพส์ตไปยังหน้ากระดานของกลุ่ม VoIP Administrator Team (VAT) โดยอัตโนมัติ ซึ่งจะบอกถึงหมายเลขไอพีต้นทางของการโจมตี ซึ่งผู้ดูแลระบบ VoIP ที่อยู่ในกลุ่ม Facebook นี้ ก็จะได้รับการแจ้งเตือนการโจมตีได้อย่างทั่วถึงและรวดเร็ว

4.3 อภิปรายผลการทดลอง

4.3.1 ชุดซอฟต์แวร์ ISANBox.F

การพัฒนาชุดซอฟต์แวร์ ISANBox.F ตามที่ได้เสนอในวิทยานิพนธ์นี้ ได้ทำการทดสอบประสิทธิภาพทั้งในด้านความมั่นคงและด้านคุณภาพการให้บริการ จากผลการทดลองพบว่าระบบมีประสิทธิภาพด้านความมั่นคงที่สูงขึ้น จากเดิมที่ซอฟต์แวร์ FreeSWITCH มีความเสียงด้านความมั่นคง คือ ถูกโจมตีด้วยการดักฟังเสียงได้ ถูกโจมตีด้วยการดักจับชื่อผู้ใช้และรหัสผ่านของหัวโทรศัพท์ได้ ถูกโจมตีตัดการติดต่อสื่อสารเพื่อยุติการสนทนาได้ และยังถูกโจมตีให้ระบบเกิดการปฏิเสธการให้บริการและทำให้ระบบล้มเหลวลงในที่สุด ซึ่ง ISANBox.F สามารถป้องกันทุกการโจมตีที่กล่าวมาในข้างต้นได้อย่างมีประสิทธิภาพ จะมีเพียงการโจมตีให้ระบบเกิดการปฏิเสธการให้บริการหรือ SIP Flooding ที่ในระบบ ISANBox.F ยังมีจุดอ่อนในเรื่องการตอบสนองของระบบตรวจจับการโจมตีที่มีความล่าช้า ซึ่งอาจทำให้การโจมตี SIP Flooding มีโอกาสเกิดขึ้นได้สำเร็จ ซึ่งวิทยานิพนธ์นี้ก็ทำการศึกษาและเสนอแนวทางแก้ไขจุดอ่อนดังกว่าไว้ในจุดระสงค์ข้อที่สองของวิทยานิพนธ์

จากผลการทดลองวัดเวลาในการใช้งานส่วนติดต่อผู้ใช้งานและส่วนการติดตั้งของทั้ง 2 ระบบ ด้วยวิธี KLM พบว่าการติดตั้งระบบ ISANBox.F ใช้เวลาลดลงจากการติดตั้ง FreeSWITCH ถึง 91.06 % และตัวอย่างการใช้งานส่วนติดต่อผู้ใช้งานในการ เปิด/ปิด การเข้ารหัสข้อมูลเสียง ในระบบ ISANBox.F ใช้เวลาลดลง จากระบบ FreeSWITCH ถึง 82.24 % สืบเนื่องมาจากส่วนติดต่อผู้ใช้งานและส่วนการติดติดตั้ง จากเดิมใน FreeSWITCH ที่ใช้ส่วนติดต่อผู้ใช้งานแบบ Text User Interface ใช้วิธีการป้อนคำสั่งผ่าน Command Line และการตั้งค่าใช้งานด้วยการแก้ไขไฟล์ XML ซึ่งเป็นวิธีที่ยุ่งยากต้องอาศัยผู้มีความรู้ และเชี่ยวชาญเฉพาะด้านจึงจะสามารถติดตั้งและใช้งานได้ อีกทั้งยังต้องใช้เวลาในการติดตั้งที่นานพอสมควร ซึ่ง ISANBox.F ได้แก้ปัญหาเรื่องความยุ่งยากในการติดตั้งใช้งานดังกล่าวโดยได้พัฒนา Web User Interface และชุดติดตั้งที่รวมเอาซอฟต์แวร์ที่จำเป็นเอาไว้ในไฟล์เดียว ทำให้เกิดความสะดวกและง่ายในการติดตั้งใช้งาน ผู้ใช้งานทั่วไปก็สามารถติดตั้งและใช้งานระบบ ISANBox.F ได้ ดังนั้นการติดตั้งใช้งานระบบ VoIP โดยการใช้ ISANBox.F จึงไม่ได้จำเป็นจะต้องเป็นผู้ใช้งานที่มีความรู้และเชี่ยวชาญเฉพาะด้านอีกต่อไป แต่อย่างไรก็ตามการประเมินเวลาในการใช้งานส่วนติดต่อผู้ใช้งานด้วยวิธี KLM ก็เป็นเพียงวิธีคำนวณเวลาจากขั้นตอนการทำงานต่างๆ ดังนั้นการทดสอบความพึงพอใจจากประสบการณ์ของผู้ใช้งานจริงก็อาจจะสะท้อนความพึงพอใจที่แตกต่างกันไป

จากผลการทดสอบประสิทธิภาพการให้บริการของระบบ ISANBox.F เปรียบเทียบกับ FreeSWITCH เห็นได้ชัดว่าเมื่ออยู่ในสภาพ Bandwidth ที่ปกติของเครือข่ายในปัจจุบันหรือที่ 100 Mbps จะพบว่าคุณภาพการให้บริการของ ISANBox.F จะไม่ลดลง คือมีคุณภาพการให้บริการอยู่ในระดับที่ผู้ใช้พึงพอใจมาก และเมื่อลด Bandwidth ลงมาที่ 10 Mbps จะทำให้คุณภาพการให้บริการหรือค่า MOS ลดลงมาเพียง 0.92 % ซึ่งยังมีคุณภาพการให้บริการในระดับที่ผู้ใช้มีความพึงพอใจ และ

ยังอยู่ในระดับที่มาตรฐาน กสทช. กำหนดคือค่า MOS มากกว่า 3.6 ได้พบประเด็นที่น่าสนใจคือ เมื่อลด Bandwidth มาที่ 5 Mbps และ 3 Mbps พบว่าคุณภาพการให้บริการของทั้ง ISANBox.F และ FreeSWITCH ตกลงต่ำกว่าที่มาตรฐานกำหนดมีค่า MOS น้อยกว่า 3.6 นั่นหมายความว่าในเครือข่ายที่ Bandwidth ต่ำมากๆ นั้น การนำเอาระบบ ISANBox.F หรือแม้กระทั้ง FreeSWITCH ไปประยุกต์ใช้งานในองค์กร ก็จะส่งผลให้ได้ระบบ VoIP ที่มีคุณภาพการให้บริการต่ำกว่ามาตรฐานกำหนด อยู่ในระดับที่ผู้ใช้งานไม่พึงพอใจต่อคุณภาพเสียง ดังนั้นนอกจากเรื่อง Overhead ของการเข้ารหัสข้อมูลเสียงที่จะมีผลต่อคุณภาพการให้บริการเพียงเล็กน้อยแล้ว เรื่องการวางแผนปรับโครงสร้าง Bandwidth ของเครือข่ายให้เหมาะสมต่อจำนวนผู้ใช้งานในองค์กร รวมทั้งเรื่องความหนาแน่นของแพ็กเก็ตในแต่ละช่วงเวลา ก็จะเป็นส่วนที่สำคัญที่จะส่งผลต่อคุณภาพการให้บริการของระบบ VoIP ด้วย

อย่างไรก็ตามจะเห็นได้ว่าการทดสอบคุณภาพการให้บริการของ ISANBox.F เป็นเพียงการทดสอบในเครือข่ายจำลอง ซึ่งสามารถควบคุมสภาพแวดล้อมของเครือข่ายจำลองนี้ได้ ไม่มีทราฟฟิกอื่นๆ เข้ามารบกวน คือทำการเชื่อมต่อภายในเครือข่าย Local Area Network (LAN) และมีผู้ใช้งาน ณ เวลาเดียวกันเพียง 15 คู่สาย อย่างไรก็ตามมีงานวิจัยที่เกี่ยวข้องของ สำเริง คำมีวงษ์ [45] ที่แสดงให้เห็นถึงคุณภาพการให้บริการของระบบ VoIP บนเครือข่ายระดับ Metropolitan Area Network (MAN) ที่มีการเพิ่มประสิทธิภาพด้านความมั่นคง จะเห็นว่าในเครือข่ายระดับ MAN ดังกล่าว โดยแม้จะมี Overhead เพิ่มขึ้นมาแต่คุณภาพการให้บริการหรือค่า MOS ก็ยังอยู่ในระดับที่ดีมากในทั้งก่อนและหลังการเพิ่มประสิทธิภาพด้านความมั่นคง ดังนั้นการนำเอา ISANBox.F ไปใช้ในเครือข่ายระดับ MAN ก็จะไม่ส่งผลต่อคุณภาพการให้บริการเช่นเดียวกัน

4.3.2 แนวทางแก้ไขปัญหา SIP Flooding

การออกแบบวิธีการแก้ไขปัญหา SIP Flooding ตามที่ได้เสนอในวิทยานิพนธ์นี้ได้ทำการทดสอบประสิทธิภาพโดยเฉพาะเรื่องการตอบสนองต่อการโจมตี ซึ่งจากผลการทดลองในเครือข่ายจำลองพบว่าวิธีการแก้ปัญหา SIP Flooding ที่ได้เสนอในวิทยานิพนธ์นี้สามารถตอบสนองต่อการโจมตีได้เร็วกว่าการวิธีการอ่านไฟล์ Log (ในกรณีที่เร็วที่สุด) ถึง 99.95 % เนื่องจากวิธีที่เสนอเป็นการตรวจจับการโจมตีโดยทำการวิเคราะห์ข้อความ Response ของโพรโทคอล SIP โดยตรง เป็นลักษณะพฤติกรรมของข้อความที่เกิดขึ้นแบบเวลาจริง (Real time) ณ เวลาขณะนั้นๆ ซึ่งจะเกิดขึ้นก่อนที่ประวัติพฤติกรรมของการส่งข้อความ Invite จะถูกบันทึกไปยังไฟล์ Log จึงทำให้วิธีการที่เสนอนี้สามารถตอบสนองได้อย่างรวดเร็ว

อย่างไรก็ตามเนื่องจากการทดสอบประสิทธิภาพของ SIP Proxy ต้นแบบนั้นได้ทดสอบอยู่บนเครือข่ายจำลอง (Test-Beds) วิทยานิพนธ์จึงได้เลือกใช้ค่าขีดแบ่ง (Threshold) ในการจำแนกการโจมตีแบบคงที่ โดยตั้งค่าขีดแบ่งที่เหมาะสมและถูกต้องที่สุดสำหรับเครือข่ายจำลอง เพื่อที่จะใช้ทดสอบประสิทธิภาพในการตอบสนองการโจมตี ซึ่งได้ให้เหตุผลในการเลือกใช้ค่าขีดแบ่งไว้ในหัวข้อ 3.3.3 ดังนั้นการกำหนดค่าขีดแบ่งตามแบบที่ได้เสนอไว้ในวิทยานิพนธ์นี้ อาจจะใช้ไม่ได้ผลกับเครือข่ายแบบอื่นๆ การเลือกใช้ค่าขีดแบ่งที่ถูกต้องและเหมาะสมยังคงเป็นประเด็นปัญหาใหญ่ของกลุ่มนักวิจัย เนื่องจากการเลือกใช้ค่าขีดแบ่งที่ไม่ถูกต้องหรือไม่เหมาะสมนั้นก็จะทำให้กระบวนการตรวจสอบการโจมตีนั้นผิดพลาดได้ตัวอย่าง เช่น ในกรณีที่มีการตั้งค่าขีดแบ่งต่ำเกินไปก็อาจจะส่งผลให้ผู้ใช้งานที่อาจจะเกิดความผิดพลาดหรือสับสนกดโทรออกติดต่อกันหลายๆ ครั้งถูกระบบตรวจจับว่าเป็นการโจมตีแล้วก็ถูกปฏิเสธการให้บริการ หรือในทางตรงกันข้ามกรณีที่ตั้งค่าขีดแบ่งสูงเกินไป ก็อาจจะทำให้การ

โจมตีนั้นหลุดรอดไปได้ทำให้ระบบล้มเหลวและปฏิเสธการให้บริการได้เช่นกัน จะเห็นได้ว่าการตั้งค่าขีดแบ่งแบบคงที่นั้นอาจไม่ใช่วิธีที่ดีที่สุดในการเลือกใช้ค่าขีดแบ่ง ซึ่งการศึกษาวิจัยเรื่องค่าขีดแบ่งที่ดีนั้นก็ไม่ได้อยู่ในขอบเขตการศึกษาของวิทยานิพนธ์นี้ จากการศึกษาเพิ่มเติมพบว่ามีงานวิจัยของ Chaisamarn และ Okuda [46] ที่ได้เสนออัลกอริธึม โมเดลในการกลั้นกรองผู้ใช้งานที่น่าเชื่อถือ รวมทั้งใช้หลักทางสถิติเพื่อกำหนดค่าขีดแบ่งในการจำแนกการโจมตี SIP Flooding ให้มีคุณสมบัติสามารถปรับค่าตัวเองให้เหมาะกับเครือข่ายแบบต่างๆ ได้อย่างอัตโนมัติ (Automatic Adaptive Threshold) ซึ่งงานวิจัยดังกล่าวก็ยังเป็นเพียงแนวคิดการออกแบบที่ยังไม่ถูกนำไปประยุกต์ใช้ในระบบใดอย่างจิงจัง

แนวทางแก้ไขปัญหา SIP Flooding ตามที่วิทยานิพนธ์นี้เสนอจะมีประสิทธิภาพด้านการตอบสนองต่อการโจมตีที่รวดเร็วขึ้น โดยมุ่งแก้ไขปัญหาการโจมตี SIP Flooding ที่มีการโจมตีมาจากแหล่งต้นทางเดียว Denial of Service (DoS) แต่ยังมีจุดอ่อนในการป้องกันการโจมตีแบบอื่น เช่น ในงานวิจัยของ Abhishek และ Santhi [47] ที่ได้เสนอรูปแบบการโจมตีในลักษณะที่ผู้โจมตีมีการตั้งค่าการส่งข้อความ Invite ในอัตราที่ต่ำ (Low Rate Attack) เพื่อหลบหนีการตรวจจับ และกระจายการโจมตีมาจากหลายๆ แหล่งพร้อมๆ กัน Distributed Denial of Service (DDOS) ซึ่งการโจมตีในลักษะดังกล่าวยังคงเป็นปัญหาในทางวิจัย เนื่องจากการตรวจจับการโจมตีในลักษณะ DDOS เป็นเรื่องที่ยุ่งยากซับซ้อนในการที่จะตรวจจับแหล่งการโจมตี เพราะการโจมตีลักษณะดังกล่าวจะมีลักษณะและพฤติกรรมคล้ายกับกับกลุ่มผู้ใช้งานปกติที่เข้ามาใช้งานระบบเป็นจำนวนมากในเวลาเดียวกัน ดังนั้นถ้าหากระบบการตรวจจับไม่มีประสิทธิภาพเพียงพอ ผู้ใช้งานปกติก็อาจจะได้รับการปฏิเสธการให้บริการที่เกิดจากการตรวจจับการโจมตีผิดพลาด หรือระบบถูกโจมตีได้สำเร็จเนื่องจากการโจมตีนั้นหลุดรอดการตรวจจับไปได้ ดังนั้นจะเห็นได้ว่าปัญหาการโจมตี SIP Flooding ในแบบ Low Rate Attack และ แบบ DDOS ยังคงเป็นปัญหาใหญ่ที่กลุ่มนักวิจัยทางด้านความมั่นคงบนเครือข่ายคอมพิวเตอร์จะได้ศึกษาวิจัยและหาวิธีแก้ไขปัญหาดังกล่าวต่อไป

กระบวนการหลังจากที่โพรโทคอล SIP ตรวจพบการโจมตีแล้ว วิทยานิพนธ์นี้จึงได้ออกแบบ Remedy Script นั่นหมายถึง Script ที่มีความยืดหยุ่น สามารถปรับแต่งแก้ไขให้สามารถเรียกใช้ฟังก์ชันต่างๆตามต้องการ โดยอันดับแรกคือเรียกใช้ฟังก์ชัน Iptables ให้บล็อกการโจมตีเพื่อป้องกันการโจมตีในทันทีที่ตรวจพบ นอกจากนั้นใน Remedy Script ยังสามารถพัฒนาให้มีฟังก์ชันต่างๆ เพิ่มเติมได้ตามต้องการ เช่น ฟังก์ชันการแจ้งเตือนทาง SMS ทางอีเมล หรือทางโซเชียลมีเดียต่างๆ ซึ่งวิทยานิพนธ์นี้ได้ให้ความสำคัญในการรายงานการโจมตีและแจ้งเตือนการโจมตีไปยังผู้ดูแลระบบอย่างรวดเร็วและทั่วถึงดังนั้นใน SIP Proxy ต้นแบบจึงได้พัฒนาให้ Remedy Script มีฟังก์ชันรายงานการโจมตีไปยังไฟล์ Log ของ SIP Proxy และฟังก์ชันแจ้งเตือนทางกลุ่ม Facebook ของผู้ดูแลระบบ เนื่องจากเป็นวิธีการแจ้งเตือนที่เข้าถึงผู้ดูแลระบบได้อย่างทั่วถึงและไม่มีค่าใช้จ่ายในการนำมาประยุกต์ใช้งาน

บทที่ 5

สรุปผลการวิจัย และข้อเสนอแนะ

5.1 สรุปและอภิปรายผลการวิจัย

วิทยานิพนธ์นี้ได้ตระหนักถึงการนำเทคโนโลยี Voice over Internet Protocol (VoIP) มาใช้ซึ่งส่งผลให้เกิดประโยชน์ในเรื่องการลดค่าใช้จ่ายในการโทรศัพท์และลดต้นทนขององค์กรได้อย่างมาก โดยเฉพาะซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพี (VoIP Open-source Software) ก็ได้เป็นที่นิยมของนักพัฒนาด้วยเหตุผลที่ไม่ต้องเสียค่าใช้จ่ายในเรื่องของลิขสิทธิ์และมีความยืดหยุ่นในการปรับแต่งใช้งาน ดังนั้นซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพี จึงเป็นที่นิยมสำหรับการนำมาพัฒนาต่อยอดประยุกต์ใช้งานกับองค์กรและหน่วยงานต่างๆ ในปัจจุบันมีซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพีที่เป็นที่นิยมนำมาใช้งานเช่น Asterisk [1], FreeSWITCH [2], และ Kamailo [3] เป็นต้น อย่างไรก็ตาม ซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพียังคงมีปัญหาเรื่องความมั่นคงทั้งในระดับ Signaling และในระดับ Media [4, 6] ซึ่งปัญหาเหล่านี้จะทำเกิดความเสียหายต่อองค์กรเป็นอย่างมาก ยังมีอีกหลายงานวิจัย [7-9] ที่พยายามแก้ไขปัญหาด้านความมั่นคงของซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพี มีรายงานจากเครือข่ายผู้ใช้งานซอฟต์แวร์ FreeSWITCH จากทั่วโลก [10, 11] พบว่าซอฟต์แวร์ FreeSWITCH มีประสิทธิภาพด้านการทำงานสูง มีคุณภาพการให้บริการและมีความเสถียรของระบบดีกว่าซอฟต์แวร์อื่น แต่ก็พบว่าในประเทศไทยซอฟต์แวร์ FreeSWITCH ยังไม่เป็นที่นิยมนำมาประยุกต์ใช้งานกันอย่างแพร่หลาย ยังมีอีกหลายงานวิจัย [6, 7, 28] ที่มุ่งเน้นแก้ไขปัญหาด้านความมั่นคงในระดับ Signaling Protocol โดยเฉพาะปัญหา SIP Flooding ที่เป็นปัญหาที่พบการโจมตีบ่อยกว่าการโจมตีแบบอื่นๆ โดยแก้ปัญหาด้วยการใช้เทคนิคการวิเคราะห์ไฟล์ Log ของระบบเพื่อตรวจจับการโจมตี แต่การแก้ไขปัญหารูปแบบนี้ก็ยังพบความไม่สมบูรณ์ คือการตอบสนองไม่ทันต่อเหตุการณ์การโจมตี ซึ่งส่งผลให้มีบางช่วงเวลาที่ไม่สามารถตรวจจับและป้องกันการโจมตีได้อย่างสมบูรณ์และทำให้ระบบ VoIP ล้มเหลวลงได้ ซึ่งถ้าระบบ VoIP นี้ถูกนำไปใช้ในทางธุรกิจที่มีความวิกฤตในการติดต่อสื่อสารสูง หรือธุรกิจที่มีความเข้มงวดในเรื่องความเสถียรของระบบก็อาจจะเกิดความเสียหายให้กับองค์กรหรือธุรกิจนั้นได้

วิทยานิพนธ์นี้จึงเสนอการพัฒนาต่อยอดและปรับปรุงประสิทธิภาพด้านความมั่นคงของซอฟต์แวร์ FreeSWITCH ทดสอบประสิทธิภาพความมั่นคงและวิเคราะห์คุณภาพการให้บริการ อีกทั้งได้เสนอแนวคิดการปรับปรุงวิธีการแก้ไขปัญหา SIP Flooding แบบตอบสนองทันต่อการโจมตีโดยการปรับแก้ที่โพรโทคอล SIP และทำการทดสอบประสิทธิภาพของการออกแบบแนวคิด

ผลการวิจัยและพัฒนาทำให้ได้ ISANBox.F ซึ่งเป็นชุดซอฟต์แวร์ระบบ VoIP ที่มีประสิทธิภาพด้านความมั่นคงสูง สะดวกต่อการติดตั้งและตั้งค่าใช้งาน อีกทั้งยังเป็นระบบให้บริการที่มีคุณภาพการให้บริการเป็นไปตามที่มาตรฐานกำหนด ได้แนวทางแก้ไขปัญหา SIP Flooding ซึ่งเป็นการพัฒนาปรับปรุงวิธีการแก้ไขปัญหาแบบเดิมคือการการอ่านไฟล์ Log เพื่อตรวจหาการโจมตีให้มีประสิทธิภาพมากขึ้น ซึ่งจากการประเมินประสิทธิภาพซอฟต์แวร์ SIP Proxy ต้นแบบที่นำเอาแนวคิดแก้ไขปัญหามาประยุกต์ใช้ พบว่าแนวคิดแก้ไขปัญหาที่ได้เสนอในวิทยานิพนธ์นี้ มีประสิทธิภาพในการป้องกันสูง คือ

สามารถตอบสนองการโจมตีได้แบบทันเหตุการณ์ ตอบสนองได้เร็วกว่าการอ่านไฟล์ Log แก้ปัญหาเรื่องการตอบสนองต่อการโจมตีได้อย่างสมบูรณ์ อีกทั้งยังมีระบบแจ้งเตือนการโจมตีไปยังสื่อสังคมออนไลน์ คือ กลุ่ม Facebook ของผู้ดูแลระบบ VoIP อีกด้วย สุดท้ายได้ทราบถึงคุณภาพการให้บริการของซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพีที่เป็นประโยชน์ต่อการนำซอฟต์แวร์เหล่านั้นมาประยุกต์ใช้งาน ทำให้ผู้ดูแลระบบ VoIP มีสารสนเทศที่เป็นประโยชน์ในการวางแผนจัดการระบบให้มีประสิทธิภาพด้านคุณภาพการให้บริการที่ดีที่สุด

5.2 ผลสัมฤทธิ์ของการวิจัย

ได้ระบบ ISANBox.F ซึ่งเป็นชุดซอฟต์แวร์ระบบ VoIP ที่มีประสิทธิภาพด้านความมั่นคงสูง คือสามารถป้องการดักฟังเสียง ป้องกันการตัดสายโทรศัพท์ ป้องกันการดักจับชื่อผู้ใช้และรหัสผ่านของโทรศัพท์ ป้องกันการโจมตีที่ทำให้ระบบปฏิเสธการให้บริการ สะดวกต่อการติดตั้งและตั้งค่าใช้งาน อีกทั้งยังเป็นระบบให้บริการที่มีคุณภาพการให้บริการสูงกว่าที่มาตรฐานกำหนด ช่วยลดค่าใช้จ่ายด้านการโทรศัพท์ขององค์กรที่นำระบบนี้ไปใช้งาน โดยสามารถนำไปใช้งานในหน่วยงานต่างๆ ของภาครัฐ เช่น โรงเรียน มหาวิทยาลัย ลดการนำเข้าซอฟต์แวร์จากต่างประเทศขององค์กร และลดการพึ่งพาซอฟต์แวร์ราคาแพงจากต่างประเทศ

อีกทั้งยังได้แนวทางแก้ไขปัญหา SIP Flooding ซึ่งเป็นการพัฒนาปรับปรุงวิธีการแก้ไขปัญหาแบบเดิมคือการการอ่านไฟล์ Log เพื่อตรวจหาการโจมตีให้มีประสิทธิภาพมากขึ้น ซึ่งจากการประเมินประสิทธิภาพซอฟต์แวร์ SIP Proxy ต้นแบบที่นำเอาแนวคิดแก้ไขปัญหามาประยุกต์ใช้ พบว่าแนวคิดแก้ไขปัญหาที่ได้เสนอในวิทยานิพนธ์นี้ มีประสิทธิภาพในการป้องกันสูงคือสามารถตอบสนองการโจมตีได้แบบทันเหตุการณ์แก้ปัญหาเรื่องการตอบสนองต่อการโจมตีในเครือข่ายทดลองได้อย่างสมบูรณ์ มีระบบแจ้งเตือนการโจมตีไปยังกลุ่ม Facebook ของผู้ดูแลระบบ VoIP ทำให้ได้ต้นแบบซอฟต์แวร์ที่สามารถนำไปผลิตในเชิงพาณิชย์ต่อไปได้ ซึ่งจะกระตุ้นให้เกิดการเจริญเติบโตของเศรษฐกิจไทยในด้านอุตสาหกรรมซอฟต์แวร์ของประเทศ

5.3 งานในอนาคตและข้อเสนอแนะ

ระบบ ISANBox.F ได้ถูกพัฒนาและทดสอบประสิทธิภาพในเครือข่ายทดลอง (Test-beds) เท่านั้น โดยที่ยังไม่ได้มีการนำไปทดลองใช้งานในสภาพแวดล้อมของเครือข่ายจริง ซึ่งถ้าหากมีการนำระบบไปทดลองใช้งานจริงก็อาจจะสะท้อนประเด็นปัญหาอื่นเพิ่มเติม เช่น เรื่องของคุณภาพการให้บริการที่จะขึ้นอยู่กับสภาพแวดล้อมของแต่ละเครือข่าย และในด้านความมั่นคงในเชิงลึกยังพบความไม่สมบูรณ์ของกระบวนการเข้ารหัสข้อมูลเสียงด้วยโพรโทคอล SRTP ซึ่งใช้วิธีการแลกเปลี่ยนกุญแจแบบ SDES ซึ่งยังพบความบกพร่องในวิธีการนี้เนื่องจาก SDES [48] เป็นวิธีการแลกเปลี่ยนกุญแจผ่านทางโพรโทคอล SIP ที่มีการทำงานเป็นลักษณะ Text-Based ไม่มีการเข้ารหัสกุญแจที่ส่ง ดังนั้นจึงสามารถดักจับและอ่านกุญแจที่ถูกส่งผ่านได้ อย่างไรก็ตามก็ได้มีงานวิจัย [49] ที่ได้เสนอต้นแบบวิธีการแก้ไขปัญหาของ SDES ซึ่งเป็นวิธีที่มีประสิทธิภาพในการแลกเปลี่ยนกุญแจอย่างมั่นคง ดังนั้นถ้าหากมีการนำเอาต้นแบบวิธีการแก้ไขปัญหาการส่งกุญแจของ SDES ดังกล่าวมาประยุกต์ใช้งานกับระบบ ISANBox.F ก็จะเป็นการเสริมความมั่นคงในกับระบบมากยิ่งขึ้น

เนื่องจากการออกแบบพัฒนารวมถึงการทดสอบประสิทธิภาพแนวคิดการการป้องกันการโจมตี SIP Flooding ในวิทยานิพนธ์นี้ ได้ทำในเครือข่ายทดลอง (Test-beds) เท่านั้น ซึ่งการที่จะนำไปใช้งานจริงเพื่อทดสอบประสิทธิภาพในเครือข่ายจริงได้นั้น ก็จำเป็นจะต้องนำเอาต้นแบบการป้องกันนี้มาพัฒนาเข้ากับซอฟต์แวร์เช่น FreeSWITCH หรือ Asterisk ซึ่งกระบวนการและวิธีดำเนินการจะมีความซับซ้อนในการออกแบบและพัฒนามากกว่าใน SIP Proxy ต้นแบบที่ใช้ในวิทยานิพนธ์นี้ โดยขอบเขตของวิทยานิพนธ์นี้ไม่ได้ครอบคลุมในการพัฒนาส่วนการนำไปใช้จริงดังกล่าว อีกทั้งการโจมตีด้วยเทคนิค SIP Flooding นั้นนับว่าเป็นการโจมตีที่เกิดขึ้นบ่อยครั้ง และมีรูปแบบพฤติกรรมการโจมตีที่หลากหลายและตรวจจับได้ยาก เช่น โจมตีในลักษณะ Invite Flood ที่มีการส่งข้อความ Invite มายัง SIP Proxy ในจำนวนที่มากและมีอัตราส่งเร็วกว่าปกติ จนทำให้เกิดการปฏิเสธการให้บริการของระบบ ซึ่งการตรวจจับการโจมตีในลักษณะนี้จะขึ้นอยู่กับการตั้งค่าขีดแบ่ง (Threshold) ในการจำแนกการโจมตีที่เหมาะสม (Appropriate Threshold) ซึ่งวิทยานิพนธ์นี้ได้ค่าขีดแบ่งดังกล่าวมาจากการทดลองวิเคราะห์ตามหัวข้อ 3.3.3 เพื่อหาว่าลักษณะและจำนวนของข้อความ Invite แบบใดที่ทำให้เกิดการปฏิเสธการให้บริการ ซึ่งเป็นค่าขีดแบ่งแบบคงที่ และได้นำผลการวิเคราะห์ดังกล่าวมาใช้ในการออกแบบแก้ไขปัญหา แต่ก็ยังมีรูปแบบการโจมตีอื่นที่ยากต่อการตรวจจับ เช่น การโจมตี SIP Flooding แบบอัตราต่ำ (low Rate Attack) [47] ซึ่งมีลักษณะการโจมตีที่มีการส่งข้อความ Invite มายัง SIP Proxy จำนวนน้อยๆ แต่เป็นการกระจายการโจมตีจากหลายๆ แหล่ง ซึ่งก็จะมีลักษณะคลายกับกลุ่มผู้ใช้งานทั่วไปที่เข้าใช้งานระบบในเวลาเดียวกัน ซึ่งถ้าหากใช้ค่าขีดแบ่ง แบบคงที่ตามในวิทยานิพนธ์นี้ก็อาจจะตรวจไม่พบการโจมตีแล้วทำให้ระบบล้มเหลวลงได้เช่นกัน แต่ถ้าหากมีการตั้งค่าขีดแบ่ง จำแนกการโจมตีให้สอดคล้องกับรูปแบบการโจมตีแบบอัตราต่ำ ก็อาจเกิดปัญหาความผิดพลาดในการตรวจสอบและอาจทำให้ผู้ใช้งานทั่วไปถูกบล็อกการใช้งานจากการตรวจสอบที่ผิดพลาดนี้ได้

อย่างไรก็ตามจะเห็นได้ว่าการกำหนดค่าขีดแบ่ง ในการจำแนกการโจมตีแบบคงที่นั้น ยังคงมีความไม่สมบูรณ์ เนื่องจากค่าขีดแบ่ง แบบคงที่ดังกล่าวนั้นจะไม่มีการปรับเปลี่ยนค่าตัวเองแบบอัตโนมัติ (Adaptive threshold) [46] เพื่อให้เข้ากับรูปแบบการโจมตีและบริบทของเครือข่ายแบบต่างๆ ดังนั้นหากมีการพัฒนาวิจัยและนำเอาการตั้งค่าขีดแบ่งที่สามารถปรับเปลี่ยนค่าตัวเองอย่างเหมาะสมแบบอัตโนมัติ (Adaptive threshold) มาประยุกต์ใช้กับแนวคิดแก้ไขปัญหาที่เสนอในงานวิทยานิพนธ์นี้ ก็จะทำให้ได้วิธีการแก้ไขปัญหา SIP Flooding ที่ตอบสนองทันต่อการโจมตีและสามารถตรวจสอบการโจมตี SIP Flooding ในรูปแบบต่างๆ ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

แนวทางการป้องกันการโจมตี SIP Flooding ตามที่เสนอในวัตถุประสงค์ข้อที่สองของวิทยานิพนธ์นี้ถึงแม้จะแก้ไขปัญหาประสิทธิภาพในการตอบสนองต่อการโจมตีของ ISANBox.F หรือระบบอื่นที่แก้ปัญหาด้วยการอ่านไฟล์ Log ได้เป็นอย่างดี แต่วิทยานิพนธ์นี้ก็ยังขาดการนำเอาแนวทางดังกล่าวไปพัฒนาให้สามารถใช้งานได้จริงกับ ISANBox.F เนื่องจากการปรับแก้โครงสร้างโพรโทคอล SIP ในซอฟต์แวร์ FreeSWITCH นั้นยังพบความยุ่งยาก และซับซ้อนของโครงสร้างซอฟต์แวร์อยู่มาก วิทยานิพนธ์นี้จึงได้เสนอเพียงแนวทางแก้ไขปัญหาพร้อมทั้งพัฒนาต้นแบบ SIP Proxy ขนาดเล็กขึ้นมาโดยใช้ Jain-SIP ซึ่งเป็น Java API เพื่อใช้ทดสอบประสิทธิภาพแนวทางแก้ไขปัญหาดังกล่าว ดังนั้นการนำแนวทางแก้ไขปัญหานี้ไปประยุกต์ใช้งานจริงกับระบบ ISANBox.F จึงเป็นอีกหนึ่งแนวทางที่น่าสนใจในการศึกษาและพัฒนาต่อในอนาคต

เอกสารอ้างอิง

เอกสารอ้างอิง

[1] "Asterisk". [Online]. July 2014 [Cited 9 July 2014];
Available from: http://www.asterisk.org.

[2] "FreeSWITCH". [Online]. January 2014 [Cited 9 July 2014];
Available from: http://www.freeswitch.org.

[3] "Kamailo". [Online]. May 2014 [Cited 9 July 2014];
Available from: http://www.kamailio.org.

[4] ปิยวัจน์ ค้าสบาย, สมนึก พ่วงพรพิทักษ์. "การประเมินปัญหาด้านความมั่นคงของซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพี". การประชุมวิชาการทางคอมพิวเตอร์และเทคโนโลยีสารสนเทศ CIT 2553; มหาวิทยาลัยมหิดล จังหวัดนครปฐม: หน้า 33-38.

[5] "Inviteflood tool". [Online] June 2014 [Cited 17 December 2014];
Available from: www.tool.kali.org/sniffingspoofing/inviteflood.

[6] Deng X, Lee C. "Security of VoIP SIP flooding and its Mitigation". Proceedings of New Zealand Computer Science Research Student Conference (NZCSRSC); April 2008; New Zealand: pp. 207-207.

[7] คธาวุฒิ จันบัวลา, สมนึก พ่วงพรพิทักษ์. "Extended Development of Open Source Software Package". การประชุมวิชาการงานวิจัยและพัฒนาเชิงประยุกต์ ECTI-CARD 2555; เชียงใหม่ ประเทศไทย: หน้า 58-63.

[8] "EZY IP- PBX". [Online]. February 2012 [Cited 9 July 2014];
Available from: http://voip.sit.kmutt.ac.th/index.php.

[9] "AsteriskNow" for Thai (ANT). [Online]. May 2013 [Cited 17 October 2014];
Available from: http://voip.sit.kmutt.ac.th/ant.php.

[10] "FreeSWITCH" Performance Testing. [Online]. 2012 [Cited 23 March 2014];
Available from: http://wiki.freeswitch.org/wiki/Performance_testing_and_configurations.

[11] "มี Open source VoIP อะไรให้เลือกใช้ได้บ้าง". [Online]. April 2013 [Cited 9 July 2014]; Available from: http://www.asteriskdiy.com/.

[12] Hongli Z, Zhimin G. "QoS Evaluation Based on Extend E-Model in VoIP". Proceedings of International Conference on Advancements in Computing Technology; 13-16 Feb. 2011; South Korea Phoenix Park; pp. 852-854.

[13] Radman P. "VoIP: Making Secure Calls and Maintaining High Call Quality". International Conference on Advances in Mobile Computing & Multimedia; November 2010; French: University of Cergy-Pointoise.

[14] Rozalina D, Georgive G. "Performance Analysis of QoS Parameters for Voice over IP Applications in a LAN Segment". Prooceeding of International Scientific Conference Computer Science 2008; Krakow Poland; pp. 232-237.

[15] ศุภชัย คลังทอง, พรพิมล ฉายรัสมี, สุขสันต์ พาณิชพาพิบูล. "กรณีศึกษาการเชื่อมต่อระหว่างโครงข่ายโทรศัพท์ ผ่านไอพีด้วยเลขหมายในหมวด 06 กับ โครงข่ายโทรศัพท์พื้นฐานและโครงข่ายโทรศัพท์เคลื่อนที่ในประเทศไทย". การประชุมวิชาการระดับประเทศทางด้านเทคโนโลยีสารสนเทศ NCIT 2010; ประเทศไทย. หน้า 235-239.

[16] "การสื่อสารด้วยระบบ VoIP". [Online]. 2013 [Cited 10 October 2014]; Available from: http://www.vcharkarn.com/varticle/17875.

[17] "โพรโทคอล SIP (Session Initiation Protocol)". [Online]. June 2013 [Cited 10 October 2014]; Available from: http://www.mind-tek.net/sip.php.

[18] Schulzrinne H, Rosenberg J. "Signaling for Internet Telephony". Proceedings of International Conference on Network Protocols (ICNP98); 13-16 October 1998; Austin USA; pp.298-307.

[19] Handley M, Schulzrinne H, Schooler E. And Rosenberg J. "SIP: Session Initiation Protocol". IETF, RFC 3261, 2002.

[20] "Skinny Client Control Protocol (SCCP)". [Online]. May 2013 [Cited 22 July 2014]; Available from: http://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-callmanager/69267-callstates-sccp-endpoints.html.

[21] Schulzrinne H, Casner S. "RTP: A Transport Protocol for Real-Time Applications". IETF, RFC 3550, July 2003.

[22] "ปัจจัยที่มีผลต่อ Quality of Service (QoS) ของ VoIP [Online]". May 2013 [Cited 21 September 2014]; Available from: www.sunrise.co.th/summer/ aek/VoIP/VoIP6.htm.

[23] ITU-T Recommendation P.800. "Methods for subjective determination of transmission quality". [Online]. May 2013 [Cited 4 June 2014]; Available from: www.itu.int/rec/T-REC-P.800-199608-l/en.

[24] "การวัดคุณภาพเสียงจากเครือข่ายสื่อสาร". [Online]. June [Cited 15 June 2014]; Available from: http://www.isacengineering.com/index.php?option=com_ content&task=view&id=169&Itemid=42.

[25] ITU-T Recommendation G.107. "The E-Model a computational model for use in transmission planning". [Online] [Cited 4 June 2014]; Available from: https://www.itu.int/rec/T-REC-G.107

[26] สาโรจน์ ยิ่งศักดิ์มงคล, ธนัญ จารุวิทยโกวิท. "ความจุระบบการใช้งานโทรศัพท์ผ่านอินเทอร์เน็ตบนโครงข่ายไร้สายแบบเมชประเภทกริด". การประชุมวิชาการเสนอผลงานวิจัยระดับบัณฑิตศึกษาแห่งชาติ; 23-24 ธันวาคม 2554; ขอนแก่น. มหาวิทยาลัยราชมงคลอีสาน; หน้า 128-134.

[27] "คุณภาพการให้บริการตามประกาศ กสทช". [Online] [Cited 4 June 2014]; Available from: www.standard.nbtc.go.th/index.php/qos.

[28] ประดิษฐ์ วงศ์สกุล, ปิยะณัฐ สุยังกุล, สมนึก พ่วงพรพิทักษ์. "ระบบให้บริการโทรศัพท์ผ่านอินเทอร์เน็ตแบบมั่นคงโดยการต่อยอดฟรีสวิตช์". การประชุมวิชาการทางคอมพิวเตอร์และเทคโนโลยีสารสนเทศ CIT 2555; เชียงใหม่ ประเทศไทย: หน้า 63-69.

[29] "Bluebox Project". [Online] 2014 [Cited 17 December 2014]; Available from: http://www.2600hz.org/

[30] "SRTP SDES key". [Online]. March 2011 [Cited 5 September 2014]; Available from: http://www.privatewave.com/security/security-protocols/srtp-sdes.html.

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

[32] Alexandre P, Edjair M. "Evaluating Voice Speech Quality in 802.11b Networks with VPN/IPSec". Proceedings of Wireless Communications and Mobile network 2005; Wuhan China:

[33] Card S, Moran T, Newell A. "The keystroke-level model for user performance time with interactive systems". Communications of the ACM ; 1987; Vol.23 pp. 396-410.

[34] Kieras D. "Using the Keystroke-Level Model to Estimate Execution Times". [Online].[Cited 23 June 2015]; Available from: http://www.cs.loyola.edu/~lawrie/CS774/S06/homework/klm.pdf.

[35] Puangpronpitag S. "Design and Performance Evaluation of Multicast Congestion Control for the Internet" .[Ph.D thesis]. Leeds: University of Leeds, UK ; November 2004.

[36] "PhonerLite". [Online]. [Cited 22 December 2014]; Available from: http://www.phonerlite.de/index_en.htm.

[37] "Commview". [Online]. [Cited 22 December 2014]; Available from: http://www.tamos.com/products/commview/.

[38] "Wireshark". [Online]. [Cited 22 December 2014]; Available from: http://www.wireshark.org.

[39] "Cain & Abel". [Online]. [Cited 22 December 2014]; Available from: http://www.openser.org.

[40] "Kali-Linux". [Online]. [Cited 22 December 2014]; Available from: http://www.kali.org/.

[41] "Jain-SIP". [Online]. [Cited 22 December 2013]; Available from: www.java.net/projects/jsip

[42] "Post to Facebook group with Facebook API". [Online].2014 [Cited 1 may 2015]; Available from: http://www.phpgang.com/how-to-post-into-facebook-group-with-php-using-graph-api_728.html

[43] "Sofia-SIP". [Online]. 2013 [Cited 23 March 2014]; Available from: http://wiki.freeswitch.org/wiki/Mod_sofia.

[44] "Internet Traffic Report". [Online]. May 2015 [Cited 29 may 2015]; Available from: http://www.internettrafficreport.com/.

[45] สำเริง คำมีวงษ์. "การประเมินและปรับปรุงระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ด". [การศึกษาค้นคว้าอิสระ วท.ม. เทคโนโลยีสารสนเทศบ]. มหาสารคาม: คณะวิทยาการสารสนเทศม มหาวิทยาลัยมหาสารคาม; 2558.

[46] Chaisamarn N, Okuda T. "SIP Flooding Attack Detection Using a Trust Model and Statistical Algorithms". Journal of Information Proceedings. 2014; 22; 118-129.

[47] Abhishek K, Santhi T. "A Novel Approach for Evaluating and Detecting Low Rate SIP Flooding Attack". International Journal of Computer Applications. 2011; July; 31-36.

[48] Andreasen F, Baugher M. "Session Description Protocol (SDP) Security Descriptions for Media Streams". IETF, RFC 4568, July 2006.

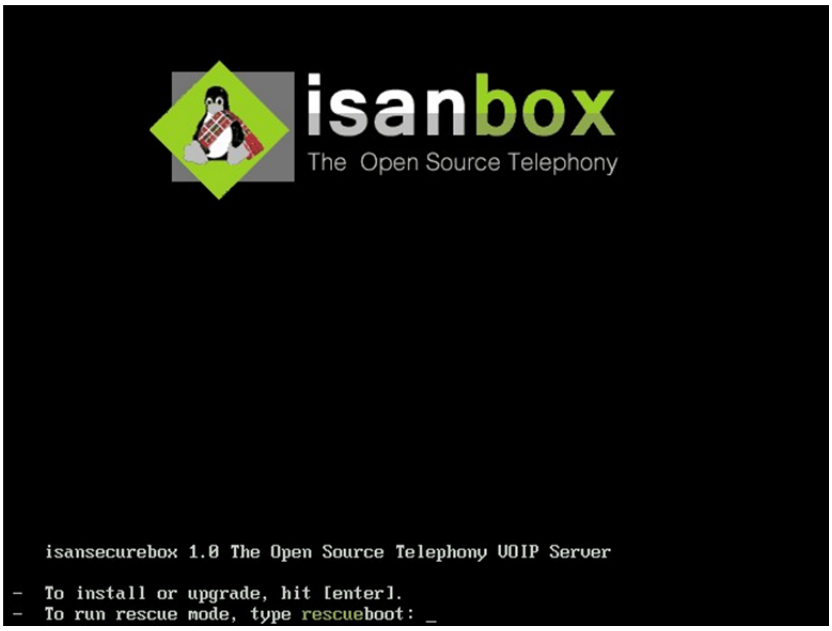
[49] Puangpronpitag S, Kasabai P. "MSDES: More SDES Key Agreement for SRTP". International Journal of Computer Theory and Engineering. 2012; October: 777-780.

ภาคผนวก

ภาคผนวก ก
คู่มือการติดตั้งระบบ ISANBox.F

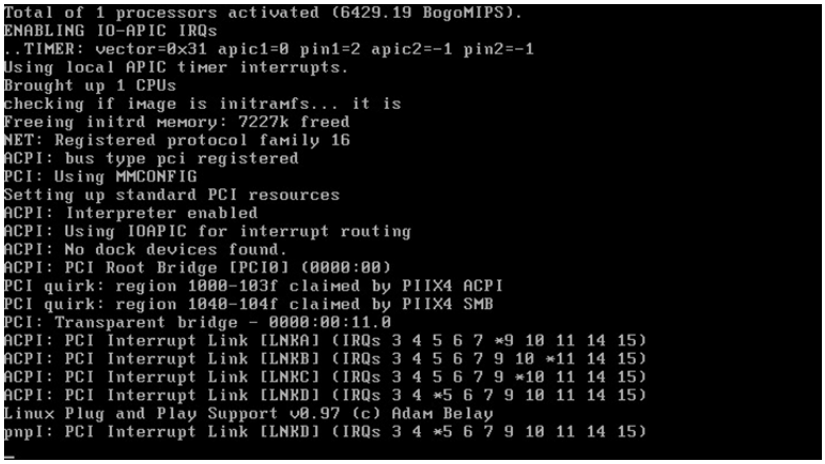
การติดตั้ง ISANBox.F

1. เมื่อใส่แผ่นติดตั้งเข้าไปแล้ว ระบบจะบูทหน้าแรกดังนี้ กด Enter เพื่อทำการติดตั้ง



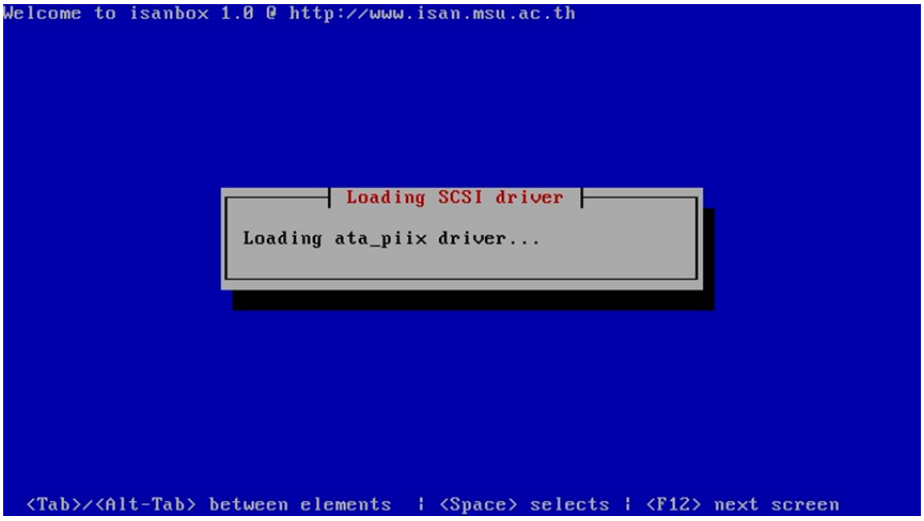
รูปที่ ก-1 Boot loader

2. ระบบจะทำการบูท ตรวจสอบอุปกรณ์ เพื่อติดตั้ง



รูปที่ ก-2 ตรวจสอบอุปกรณ์ที่เชื่อมต่อ

3. ระบบจะทำการบูทหน้าติดตั้งขึ้นมา



รูปที่ ก-3 เตรียม Driver

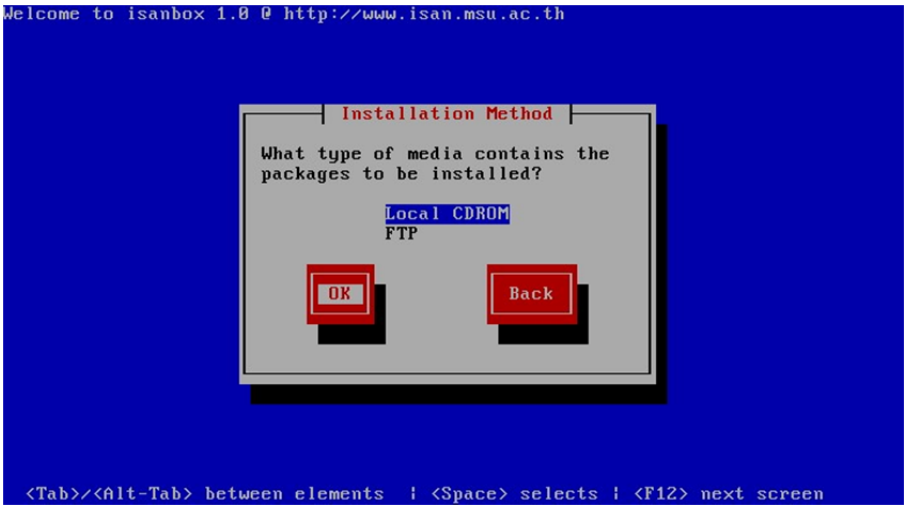
4. ทำการเลือกภาษา เป็น English กด tab เพื่อเลือก OK แล้วกด Enter

รูปที่ ก-4 เลือกภาษา

5. เลือก Keyboard เป็น US กด tab เพื่อเลือก OK แล้วกด Enter

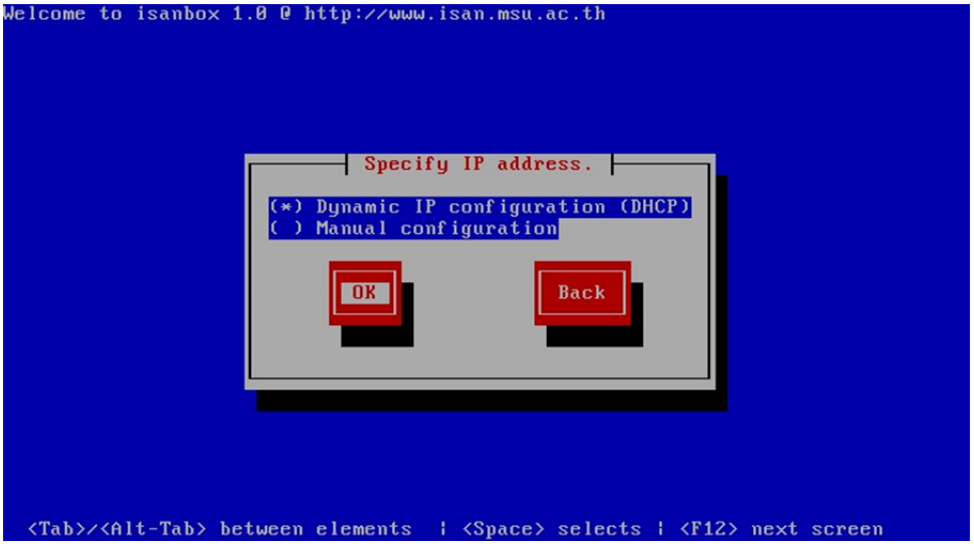
รูปที่ ก-5 เลือก Keyboard

6. เลือก Installation เป็น Local CDROM กด tab เพื่อเลือก OK แล้วกด Enter



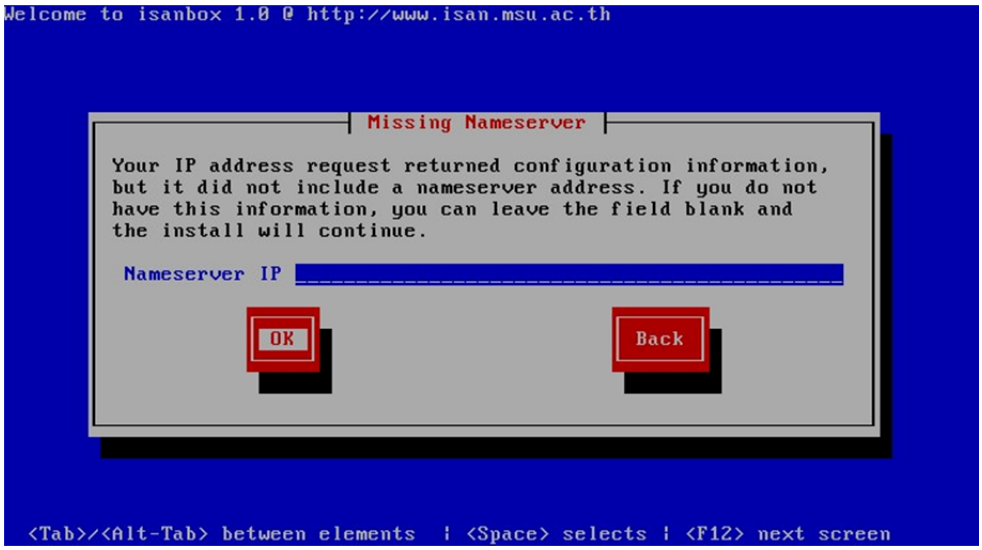
รูปที่ ก-6 เลือกรูปแบบการติดตั้ง

7. เลือก Dynamic IP configuration (DHCP) กด OK



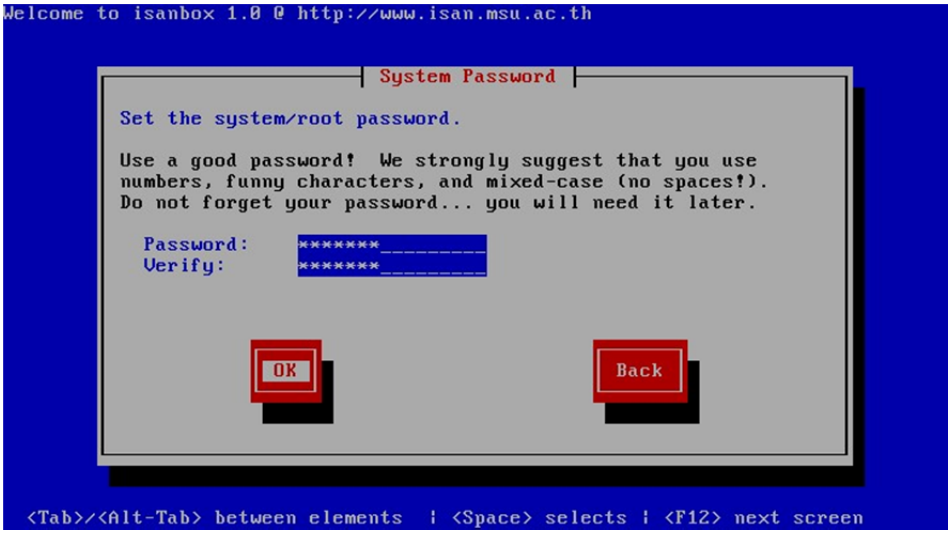
รูปที่ ก-7 เลือกรูปแบบของการตั้งค่า IP

8. ข้ามไปยัง OK แล้วกด Enter ในที่นี้ เพื่อเพราะเราจะไม่ กำหนด IP แล้วรับเป็นแบบ DHCP



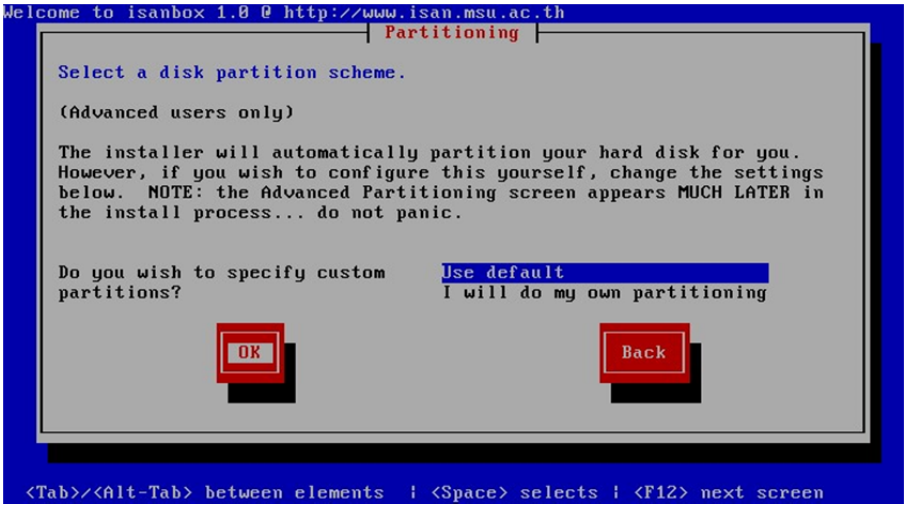
รูปที่ ก-8 กำหนด IP Server

9. ในหน้านี้จะเป็นการตั้ง Password เพื่อเข้าสู่ระบบ



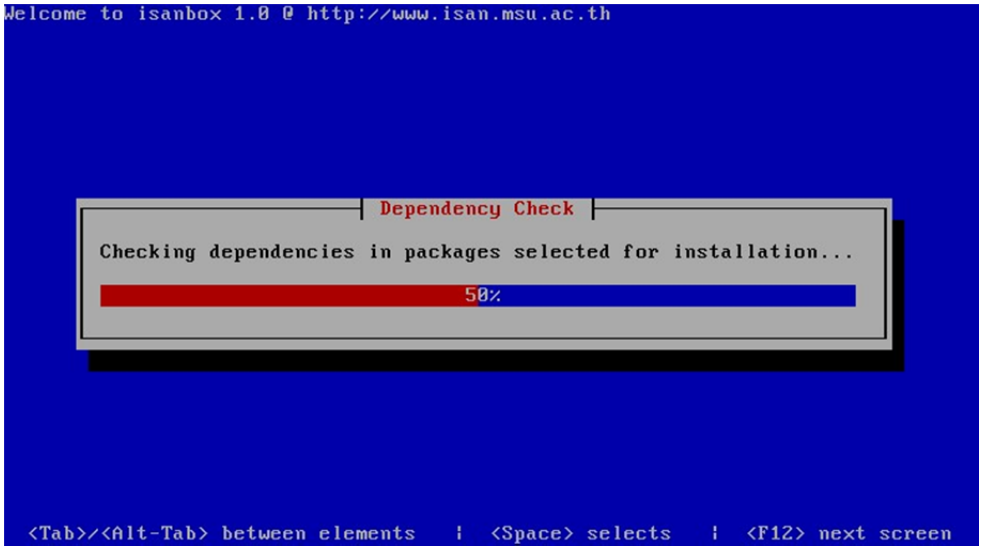
รูปที่ ก-9 รหัสผ่านในการเข้าระบบ

10. เลือก Partition เป็น Use default กด tab เพื่อเลือก OK



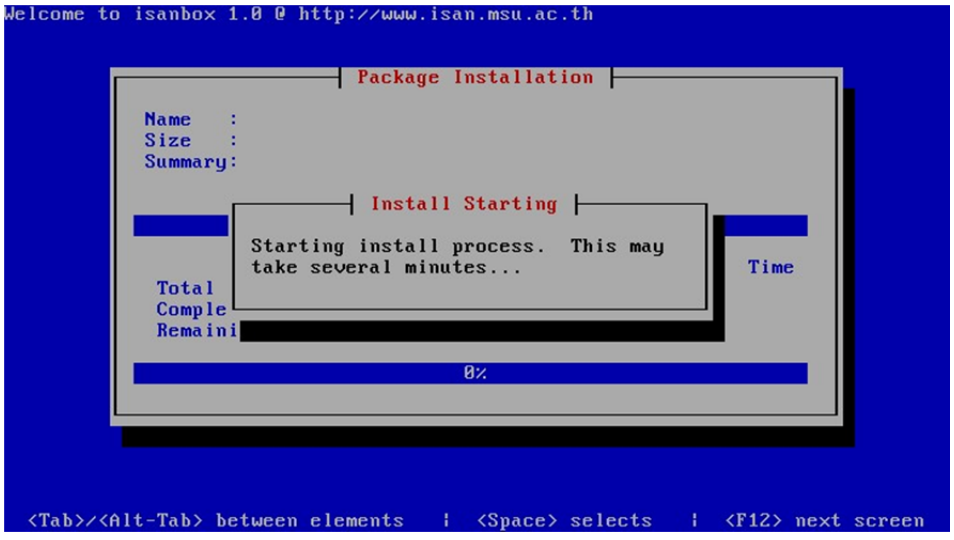
รูปที่ ก-10 กำหนดพาร์ติชั่น

11. ระบบจะทำการเช็คเพื่อติดตั้ง



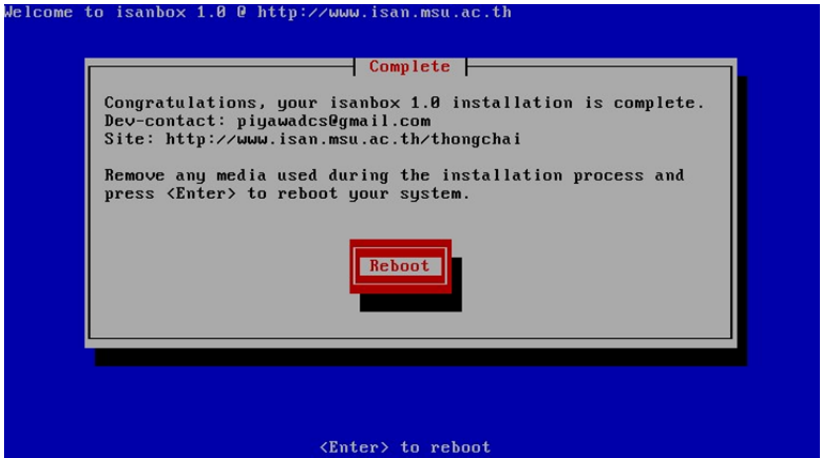
รูปที่ ก-11 ตรวจสอบความพร้อมในการติดตั้ง

12. ระบบจะทาการ ติดตั้ง Package ทั้งหมด



รูปที่ ก-12 ติดตั้ง Package

13. เมื่อติดตั้งเสร็จ ระบบจะต้องการ Reboot เลือก Reboot แล้วกด Enter

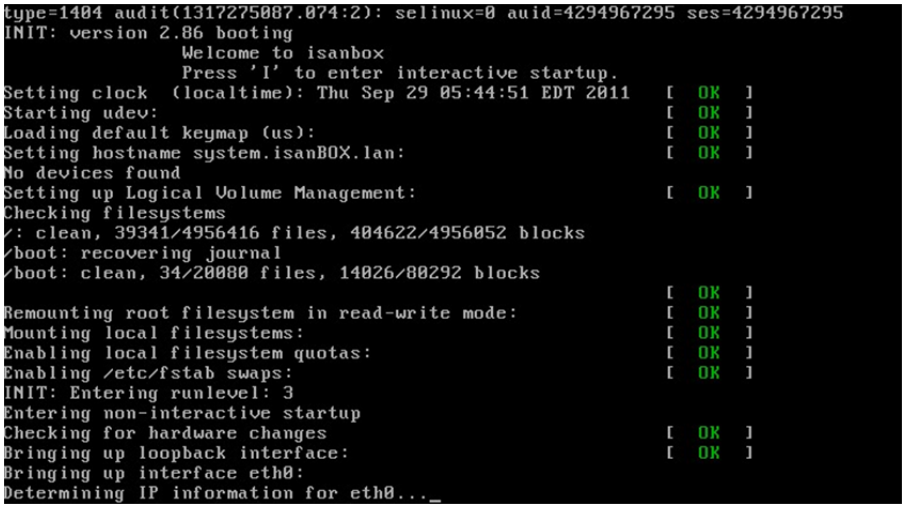


รูปที่ ก-13 Reboot ระบบ

14. เมื่อ Reboot เสร็จ ระบบจะทำการ บูทเข้าสู่ระบบปฏิบัติการ

รูปที่ ก-14 เข้าสู่ ระบบ ISANBox.F

15. ระบบจะบูท service ต่างๆขึ้นมา



รูปที่ ก-15 Start Service

16. เมื่อระบบบูทเสร็จเรียบร้อย จะเข้าสู่หน้า login จากนั้นก็ใส่ User และ Password เพื่อเข้าสู่ระบบ

รูปที่ ก-16 login user : root password : ตามที่ตั้งไว้ในภาพที่ ก-9

17. ใช้คำสั่ง ifconfig เพื่อดู IP ของ ISANBox.F

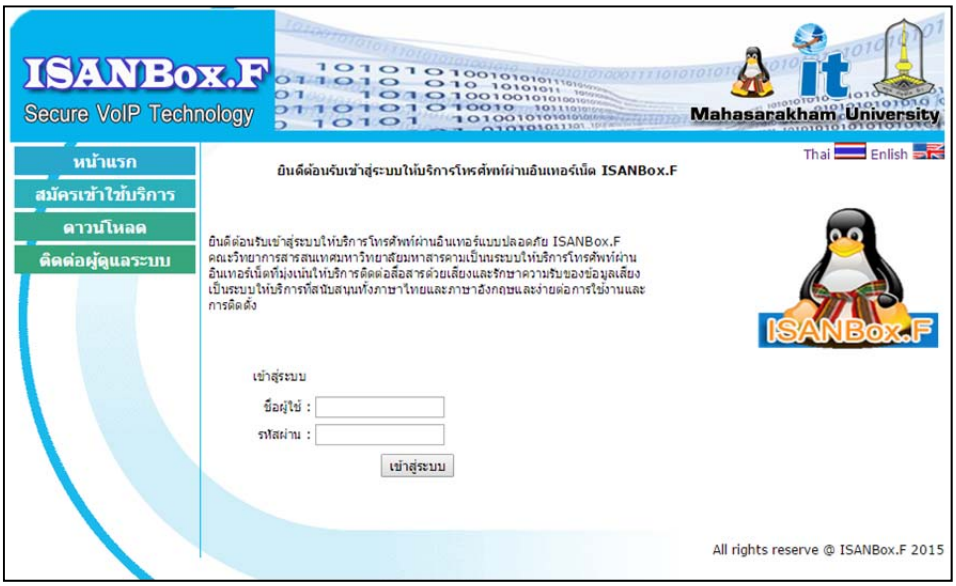
```
system login: root
Password:
Last login: Fri Oct  7 03:16:35 on tty1
[root@system ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:F8:6C:A3
          inet addr:10.31.1.83  Bcast:10.31.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fef8:6ca3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:55 errors:0 dropped:0 overruns:0 frame:0
          TX packets:17 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4062 (3.9 KiB)  TX bytes:1644 (1.6 KiB)
          Interrupt:67 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

[root@system ~]# +_
```

รูปที่ ก-17 ดูหมายเลข IP ของ Server

18. จากนั้นให้ลอง ISANBox.F เข้าใช้งานใน Browser ตรงช่อง URL ใส่ IP Server เราลงไปก็จะ เข้าสู่ระบบของ ISANBox.F เป็นอันเสร็จเรียบร้อย



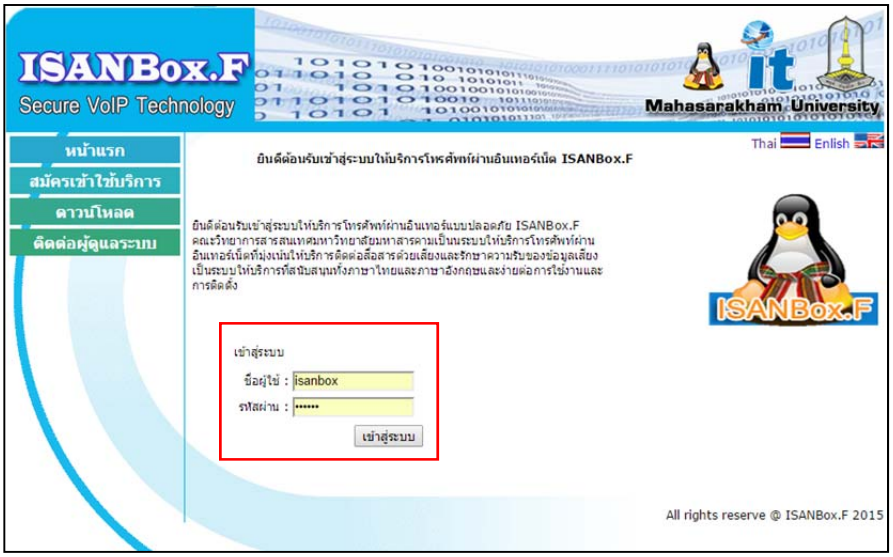
รูปที่ ก-18 หน้าจอหลักของระบบ

ภาคผนวก ข
คู่มือการใช้งานระบบ ISANBox.F

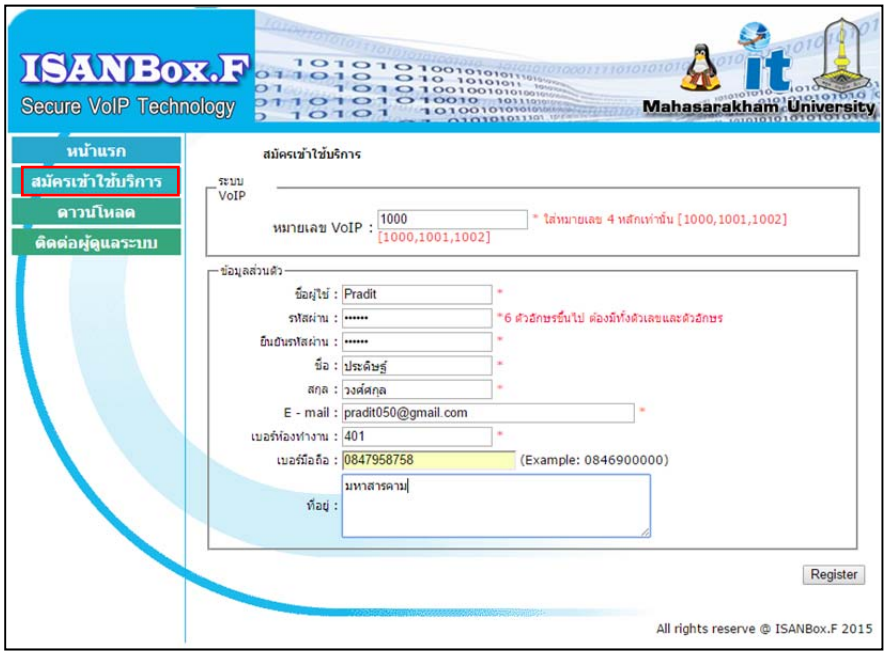
คู่มือการเข้าใช้งาน ISANBox.F

ในระบบของ ISANBox.F มีชื่อผู้ใช้ที่เป็นผู้ดูแลระบบ(ค่าเริ่มต้น)คือ isanbox รหัสผ่าน abc123 ซึ่งสามารถเปลี่ยนรหัสผ่านและข้อมูลได้ภายหลัง โดยสามารถเข้าใช้งานและจัดการระบบได้ทาง Web Browser ด้วยหมายเลขไอพีของ VoIP Server

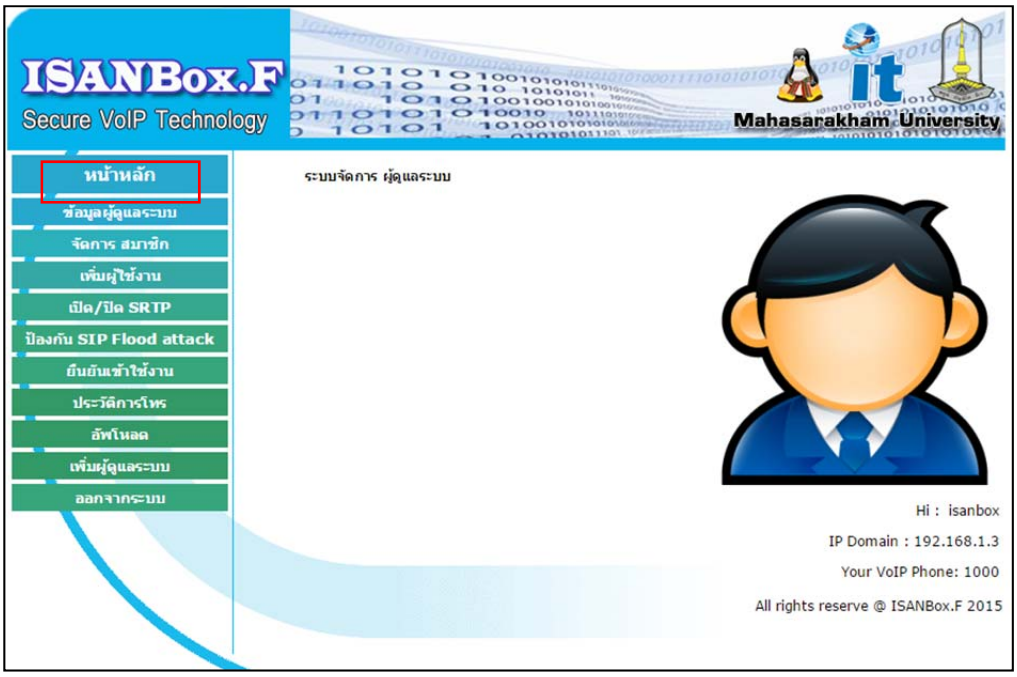
1. Administrator Mode



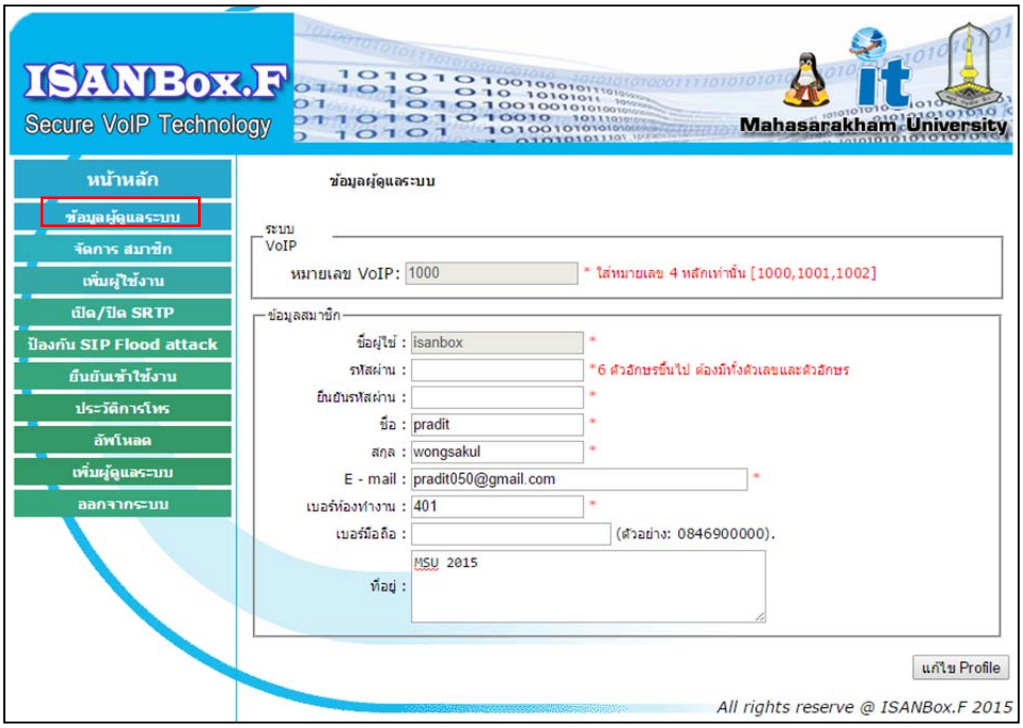
รูปที่ ข-1 Login เข้าใช้งานระบบ



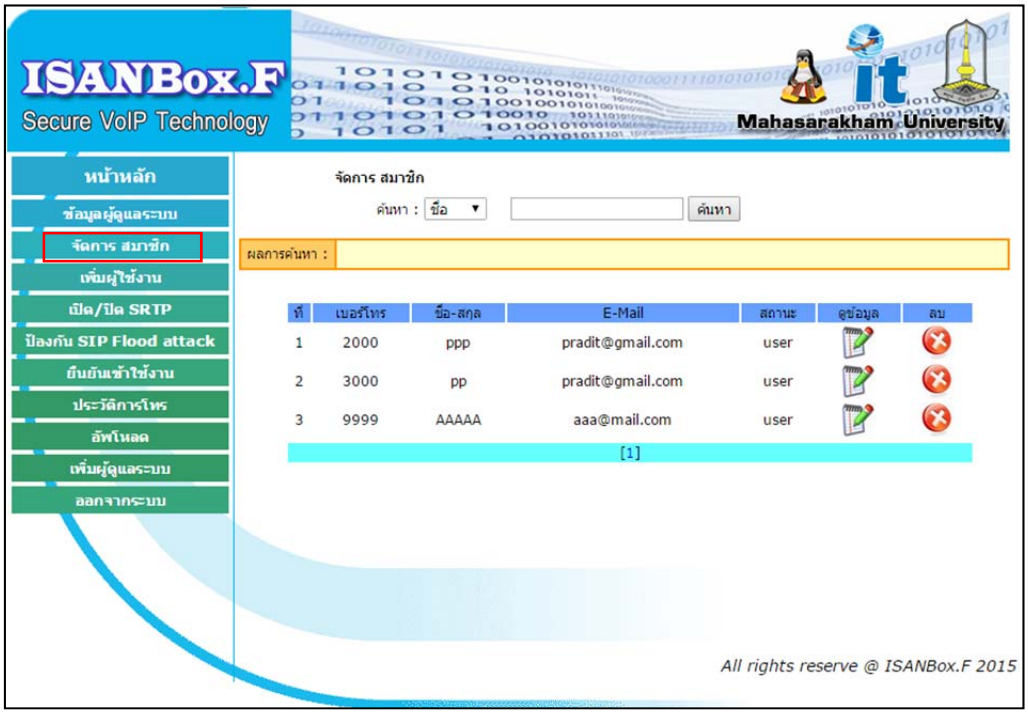
รูปที่ ข-2 การสมัครสมาชิกเข้าใช้งาน



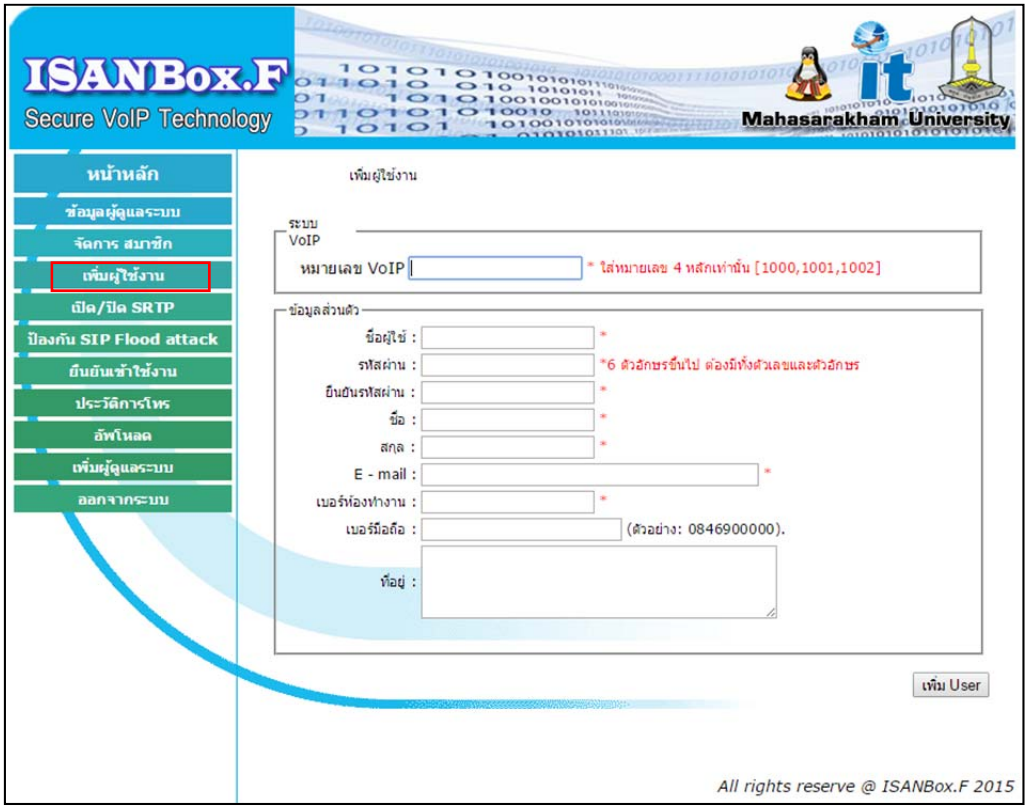
รูปที่ ข-3 หน้าจอ ผู้ดูแลระบบ



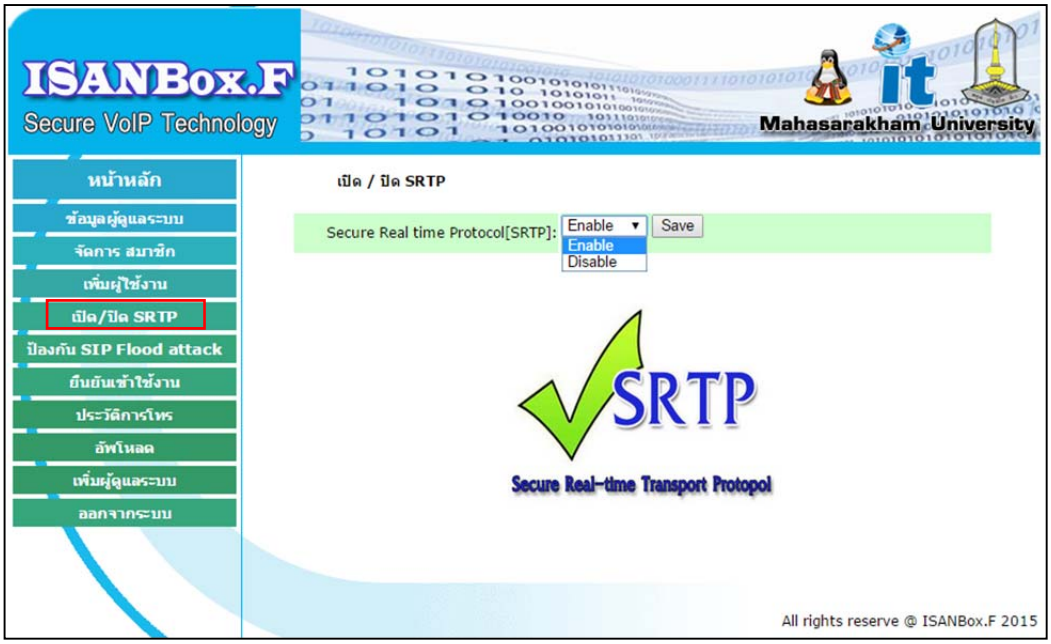
รูป ข-4 หน้าจอ ข้อมูลผู้ดูแลระบบ ผู้ดูแลระบบสามารถแก้ไขข้อมูลส่วนตัวและแก้ไขรหัสผ่านได้



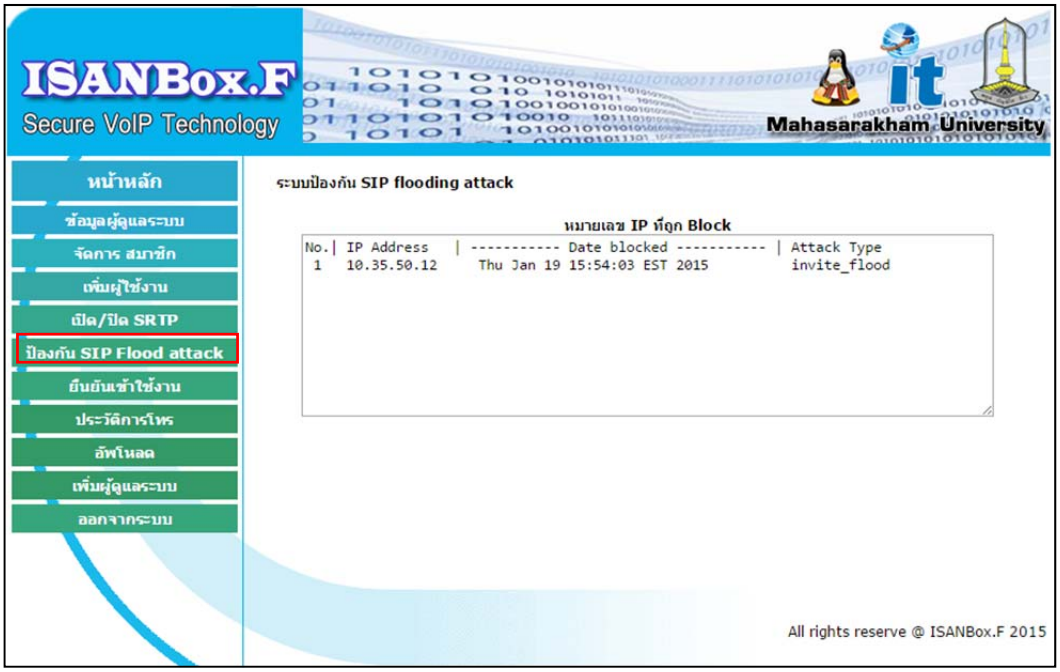
รูปที่ ข-5 หน้าจอ จัดการสมาชิก ผู้ดูแลระบบสามารถเข้าไปค้นหา ดูข้อมูล แก้ไขข้อมูลส่วนตัว แก้ไขรหัสผ่านและลบผู้ใช้งานอื่นได้



รูปที่ ข-6 หน้าจอ เพิ่มผู้ใช้งาน ผู้ดูแลระบบสามารถเพิ่มผู้ใช้งานคนอื่นๆได้

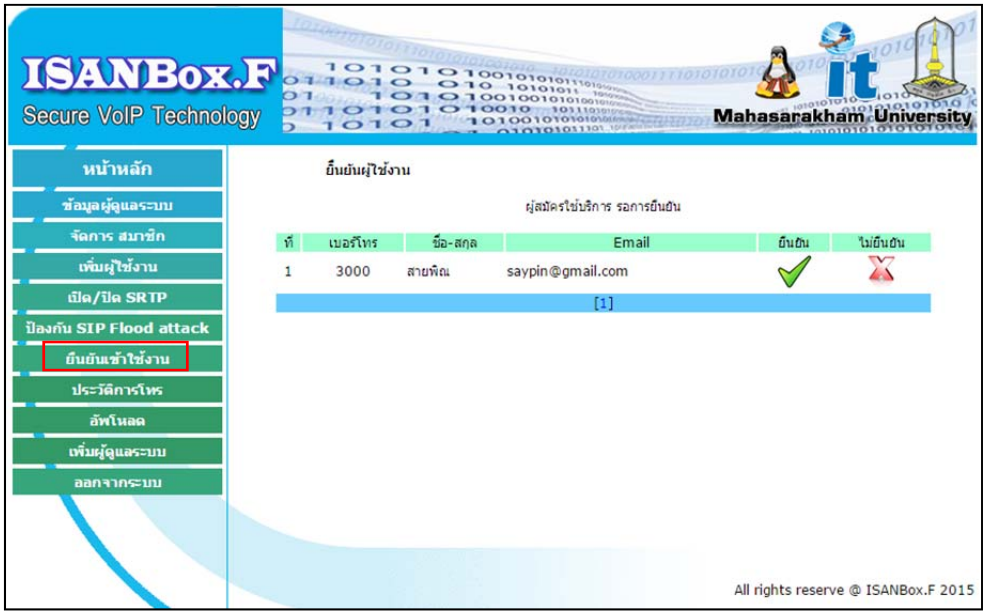


รูปที่ ข-7 หน้าจอ เปิด/ปิดการใช้งาน SRTP เพื่อเข้ารหัสข้อมูลเสียงได้

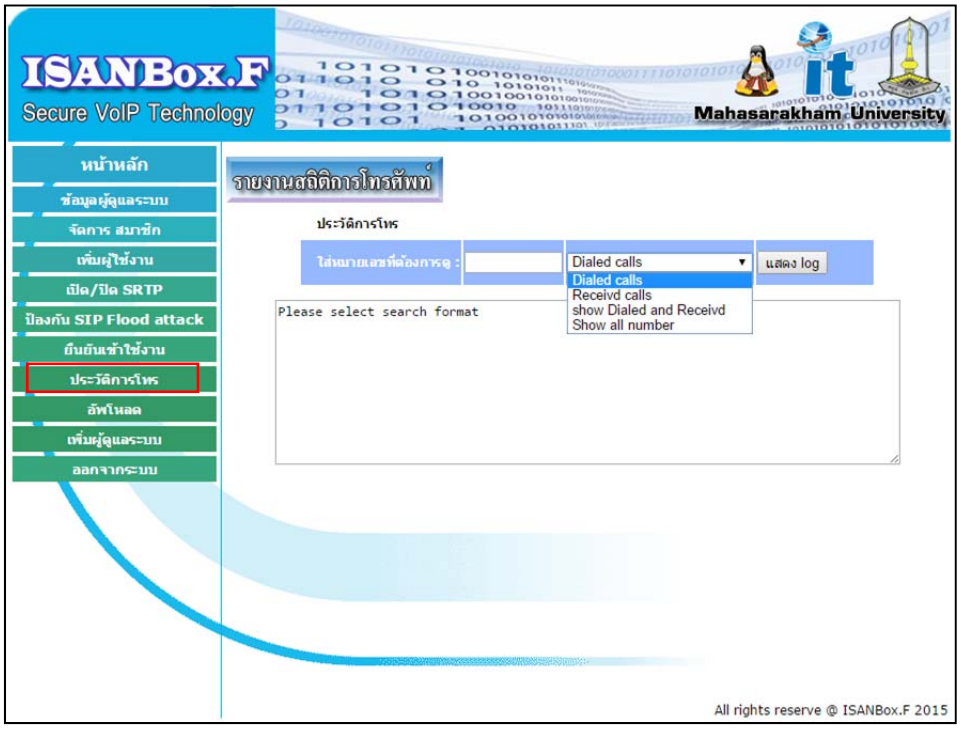


รูปที่ ข-8 หน้าจอ ป้องกันการโจมตีแบบ SIP Flooding

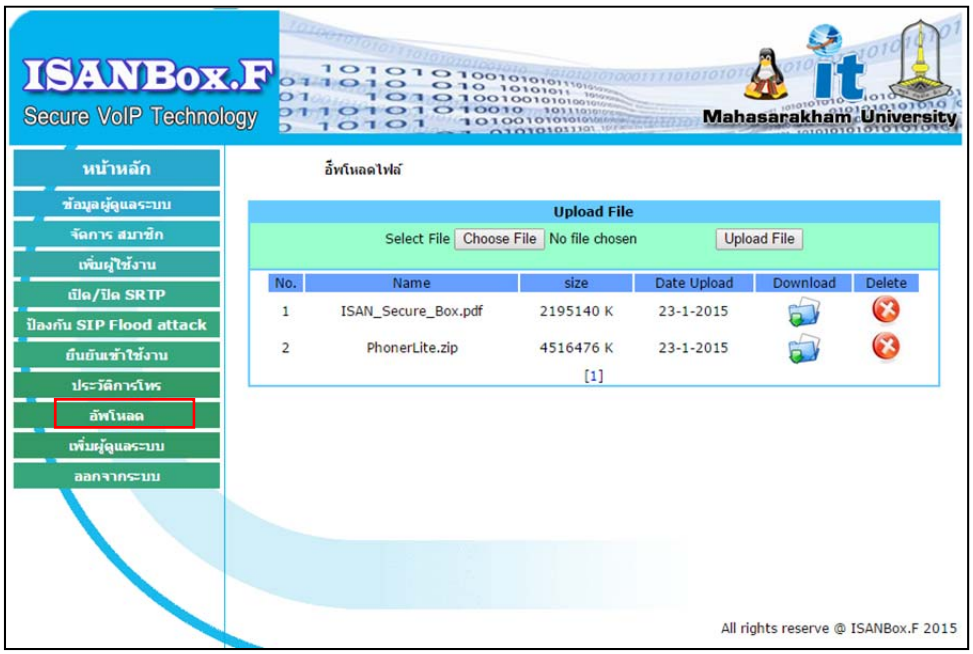
ดูแลระบบสามารถตรวจสอบการโจมตีและหมายเลขไอพีที่ถูกบล็อก และยกเลิกการบล็อกได้ โดยการยกเลิกการบล็อก IP ก็สามารถทำได้โดยการเข้าไปสั่งรันสคลิปที่ ใน VoIP Server โดยใช้คำสั่ง คือ /usr/local/freeswitch/script/unblockIP 10.35.50.12



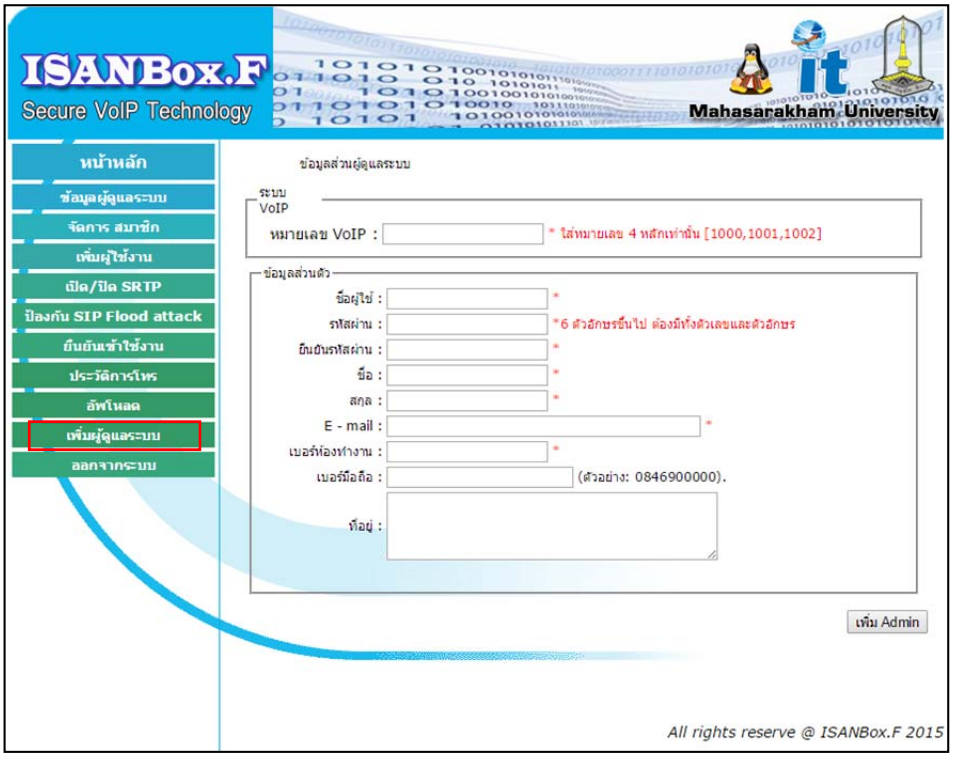
รูปที่ ข-9 หน้าจอ ยืนยันการเข้าใช้งานผู้ดูแลระบบสามารถอนุญาตหรือไม่อนุญาตให้กับผู้ใช้งานที่สมัครเข้ามาใหม่



รูปที่ ข-10 หน้าจอ ประวัติการโทร ผู้ดูแลระบบสามารถตรวจสอบประวัติการโทรของแต่ละ

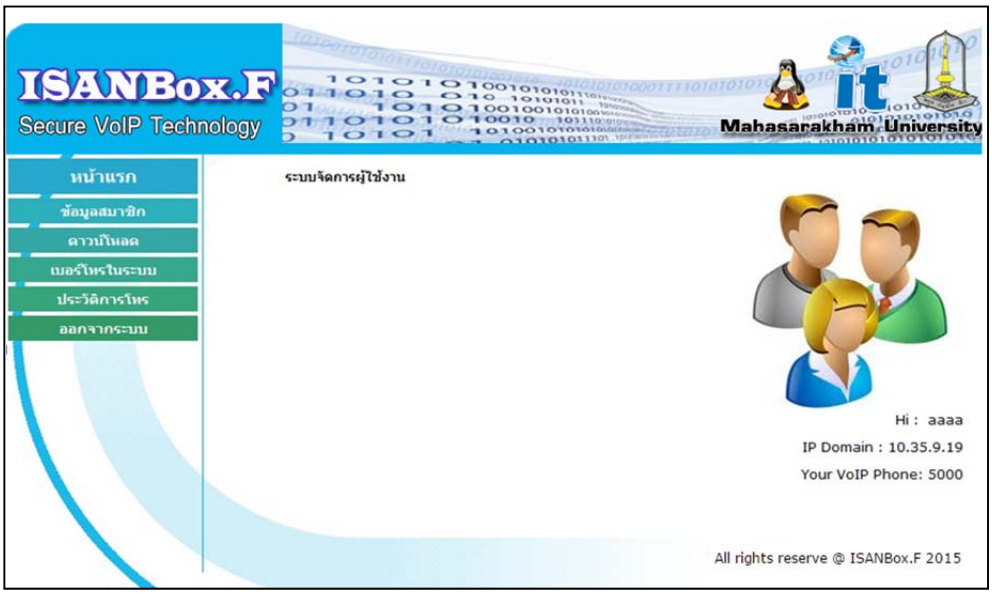


รูปที่ ข-11 หน้าจอ อัพโหลดไฟล์ ผู้ดูแลระบบสามารถอัพโหลดไฟล์และลบไฟล์ได้

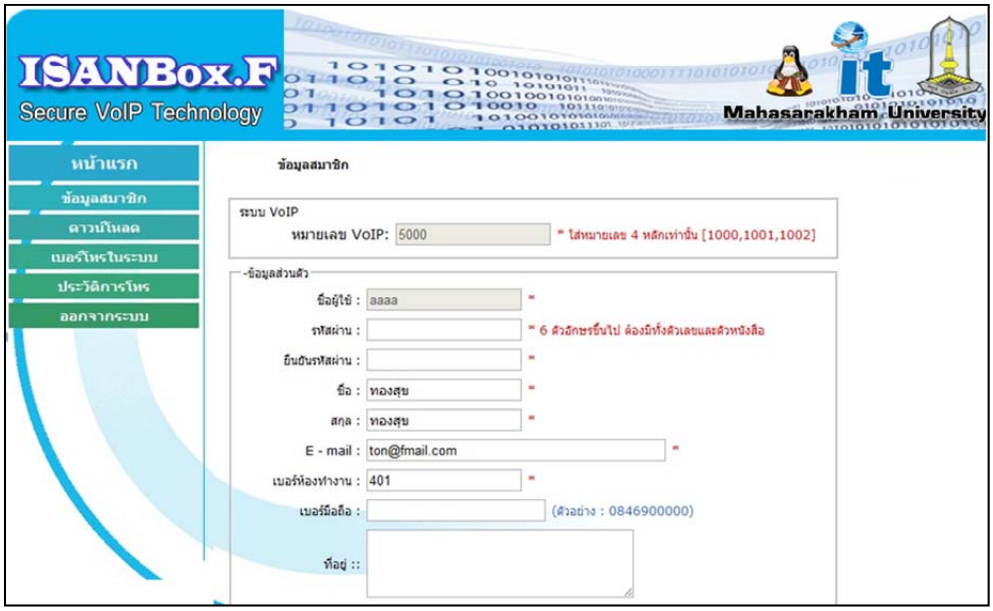


รูปที่ ข-12 หน้าจอ เพิ่มผู้ดูแลระบบ ผู้ดูแลระบบ สามารถเพิ่มและลบ ผู้ดูแลระบบคนอื่นๆ ได้

2. User Mode ในส่วนของ User Mode เป็นส่วนของผู้ใช้งานทั่วไปในระบบของ ISANBox.F ที่จะเข้ามาดู ข้อมูล แก้ไข ข้อมูลของตัวเองได้ ค้นหาเบอร์โทรที่มอยู่ในระบบ

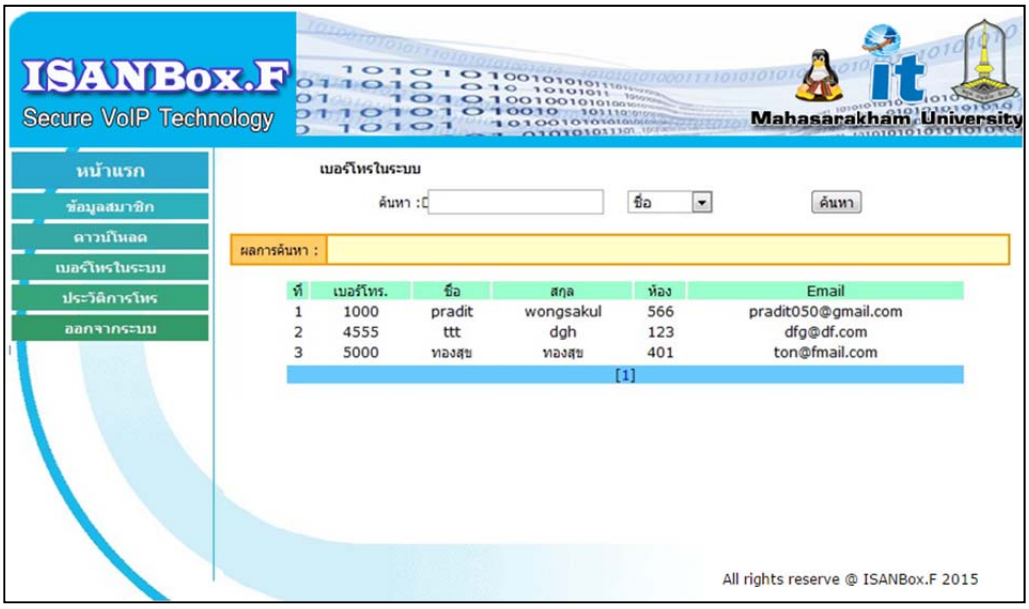


รูปที่ ข-13 หน้าจอ ผู้ใช้งาน

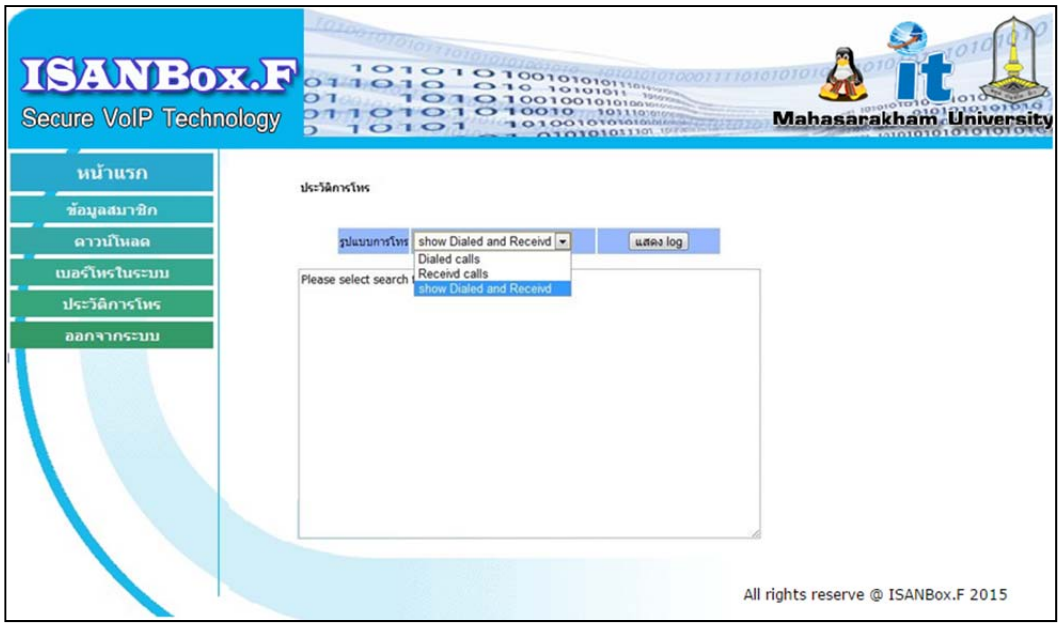


รูปที่ ข-14 หน้าจอ ข้อมูลผู้ใช้งาน ผู้ดูแลระบบสามารถแกไขข้อมูลส่วนตัวและแก้ไขรหัสผ่านได้

รูปที่ ข-14 หน้าจอดาวน์โหลดผู้ใช้งานสามารถ Download เอกสาร คู่มือการใช้งานหรือโปรแกรมได้



รูปที่ ข-15 หน้าจอ เบอร์โทรในระบบ ผู้ใช้งานสามารถค้นหาเบอร์โทรในระบบได้



รูปที่ ข-16 หน้าจอ ประวัติการโทร ผู้ใช้งานสามารถดูประวัติการโทรของตัวเองได้

ภาคผนวก ค
การติดตั้งโปรแกรม PhonerLite การตั้งค่าเพื่อใช้งาน SRTP และการตั้งค่า SIP TLS

การติดตั้งโปรแกรม PhonerLite และการตั้งค่าเพื่อใช้งาน SRTP ตั้งค่า SIP TLS

เนื่องจากระบบต้องใช้ Soft phone ในการติดต่อสื่อสารซึ่งต้องทาการลงไว้ที่เครื่อง Client ซึ่งมีวิธีการติดตั้งดังนี้

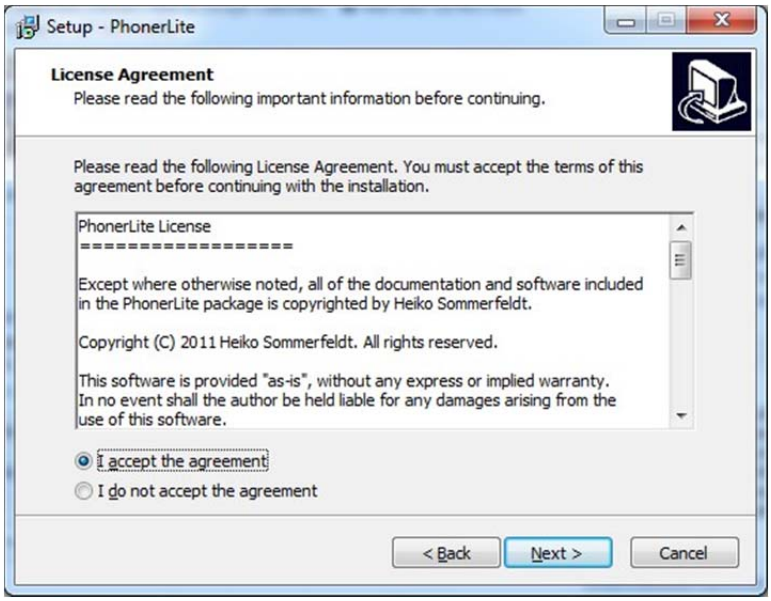
1. เมื่อคลิกติดตั้งไฟล์ PhonerLiteSetup.exe จะได้หน้าต่างเพื่อให้เลือกภาษาจากนั้นทาการเลือกภาษาอังกฤษ แล้วกด OK

รูปที่ ค-1 เลือกภาษาในการติดตั้ง

2. กดปุ่ม Next

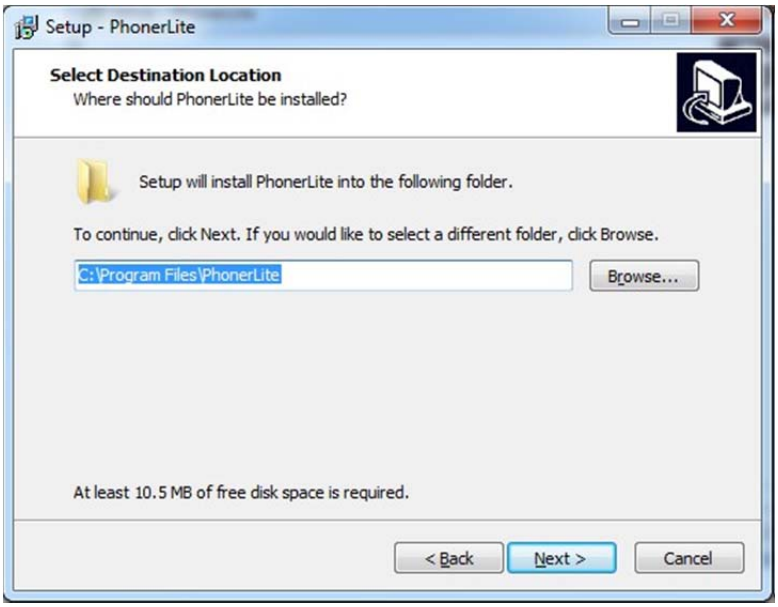
รูปที่ ค-2 ข้อมูลของโปรแกรม PhonerLite

1. เลือก I accept the agreement เพื่อยอมรับเงื่อนไขการใช้งาน และกด Next



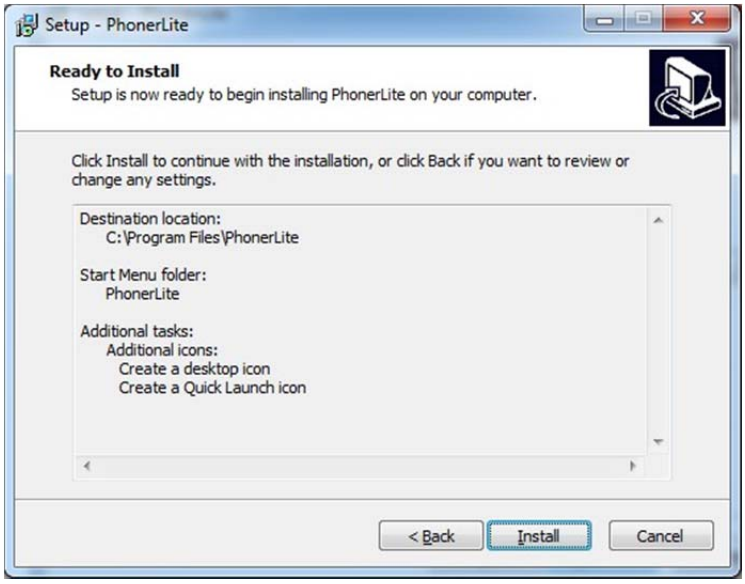
รูปที่ ค-3 ยอมรับเงื่อนไขการใช้งาน

2. เลือกตำแหน่งของแฟ้มที่จะติดตั้ง และกด Next



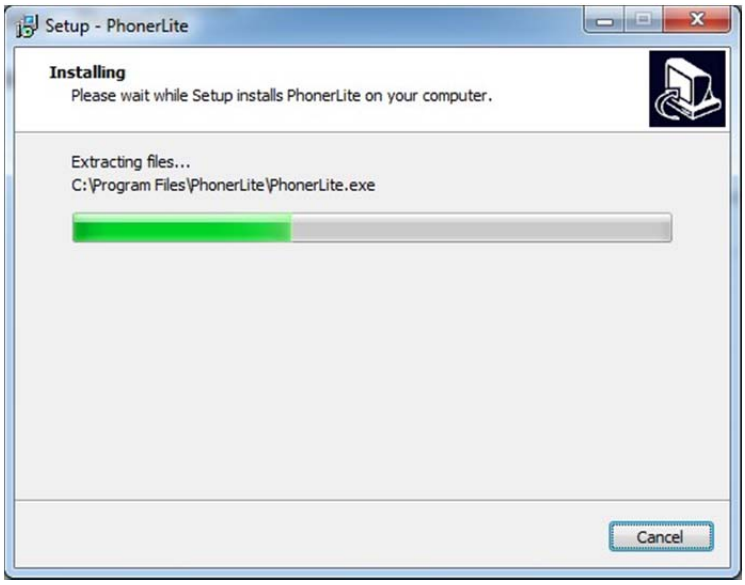
รูปที่ ค-4 เลือกที่ตั้งไฟล์ที่จะติดตั้ง

3. แสดงรายระเอียดการติดตั้งก่อนติดตั้ง กด Install เพื่อติดตั้ง



รูปที่ ค-5 รายละเอียดการติดตั้ง

4. รอการติดตั้ง



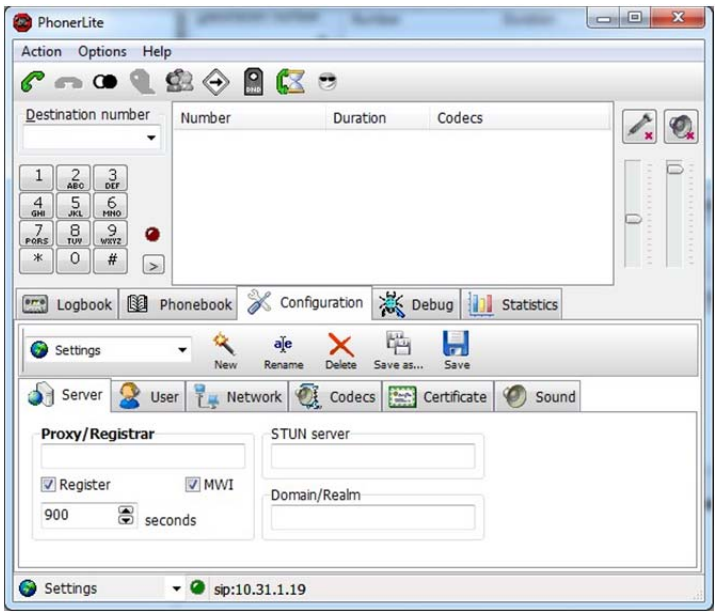
รูปที่ ค-6 ความคืบหน้าการติดตั้ง

5. ติดตั้งเสร็จเรียบร้อย กด Finish เพื่อเริ่มใช้งาน PhonerLite

รูปที่ ค-7 ติดตั้งเสร็จสมบูรณ์

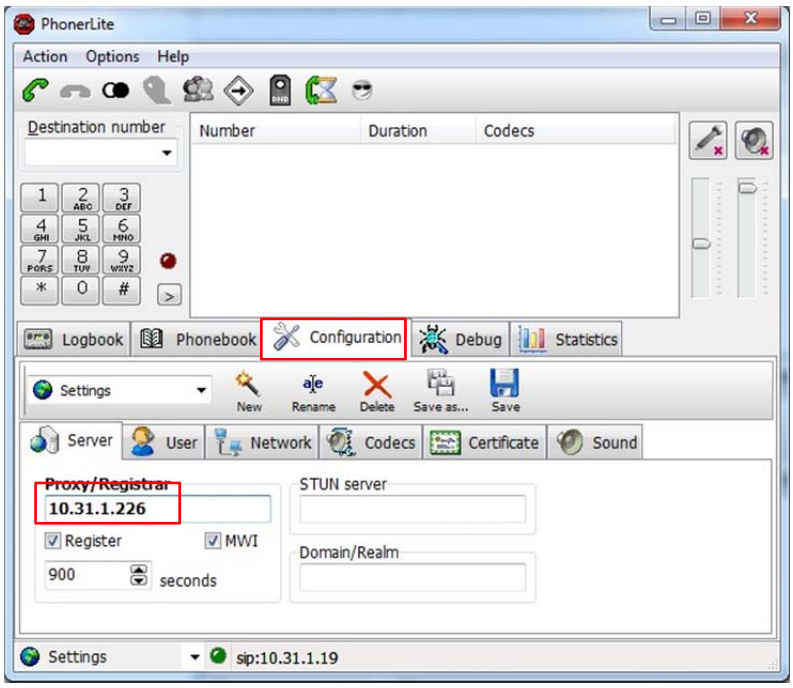
เมื่อทาการติดโปรแกรมเสร็จเรียบร้อยให้เปิดโปรแกรมขึ้นมาเพื่อที่ตั้งคาการใช้งานการโทรและใช้ SRTP ตามขั้นตอนวิธต่อไปนี้

6. เมื่อเริ่มทำงานโปรแกรม PhonerLite จะได้หน้าต่างโปรแกรมซึ่งต้องตั้งค่า SIP User และ IP ของServer



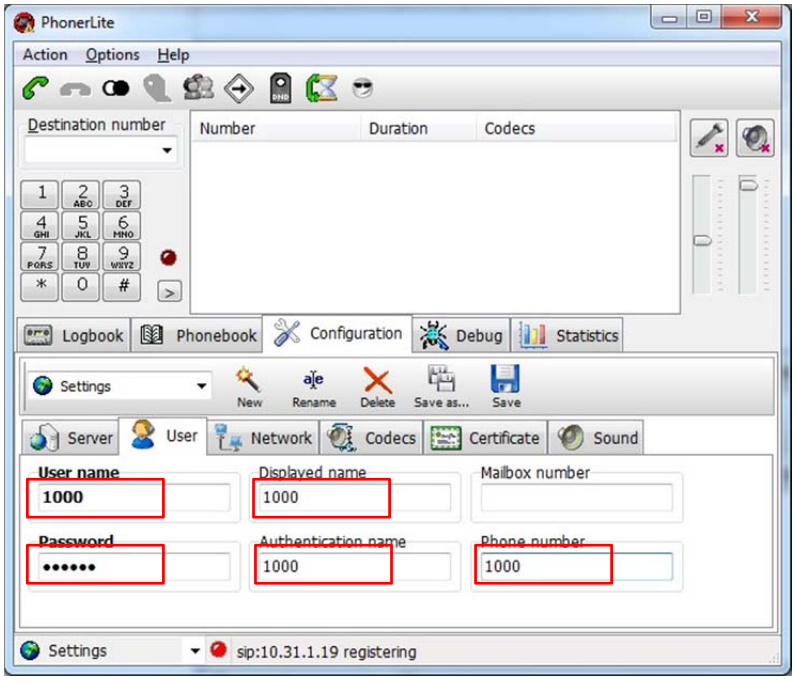
รูปที่ ค-8 หน้าต่างโปรแกรม PhonerLite

7. เลือกที่แท็บ Configuration แล้วไปที่ Server จากนั้นใส่หมายเลข IP ของ Server



รูปที่ ค-9 ตั้งค่า IP Server

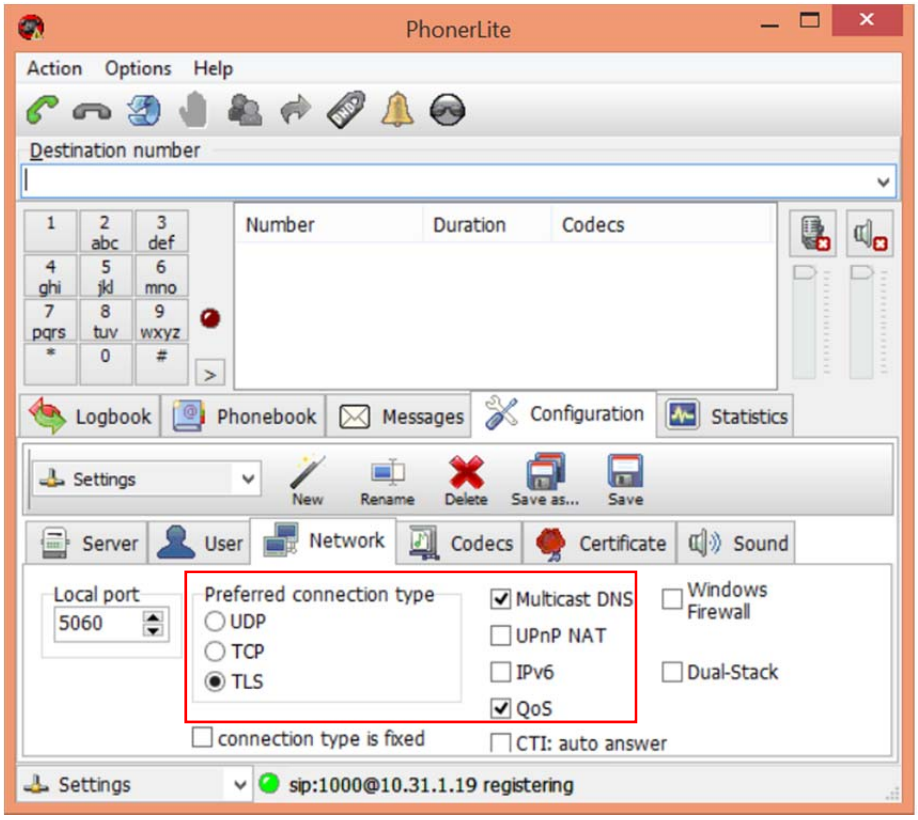
8. จากนั้นไปที่แท็บ User แล้วตั้งค่า SIP User ดังนี้



รูปที่ ค-10 ตั้งค่า SIP User

- ในช่องของ User name ให้ใส่ หมายเลขโทรศัพท์ที่ได้สมัครไว้ 1000
- ในช่อง Display name ให้ใส่ หมายเลขโทรศัพท์ที่ได้สมัครไว 1000
- ในช่อง Authentication name ให้ใส่ หมายเลขโทรศัพท์ที่ได้สมัครไว 1000
- ในช่อง Phone Number ให้ใส่ หมายเลขโทรศัพท์ที่ได้สมัครไว้ 1000
- ในช่อง Passsword ให้ใส่รหัสผ่านที่สมัครไว้กับระบบโทรศัพท์

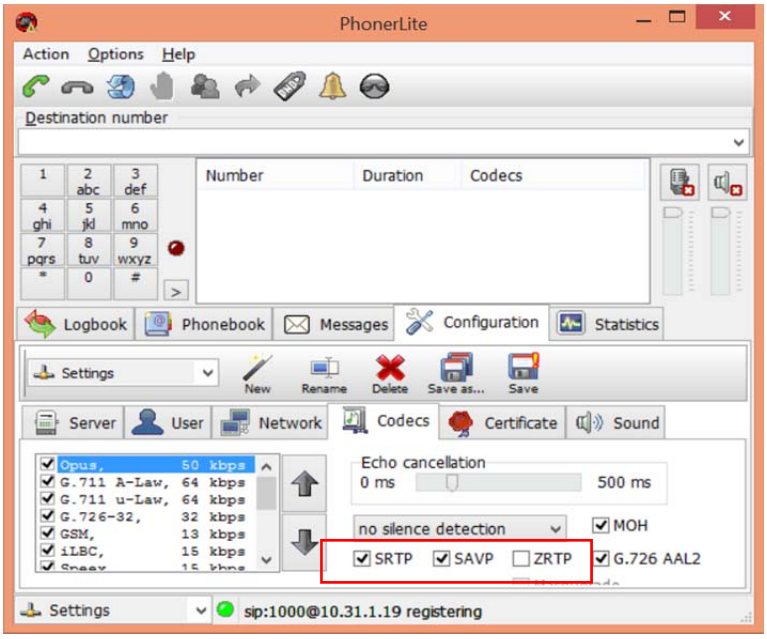
9. จากนั้นไปที่แท็บ Network แล้วตั้งค่าระบบทำงานดังนี้



รูปที่ ค-11 ตั้งค่า ระบบทางาน

- เลือก Local port เป็น 5060
- เลือก Preference connection type เป็น TLS
- เลือก Multicast DNS และ QoS

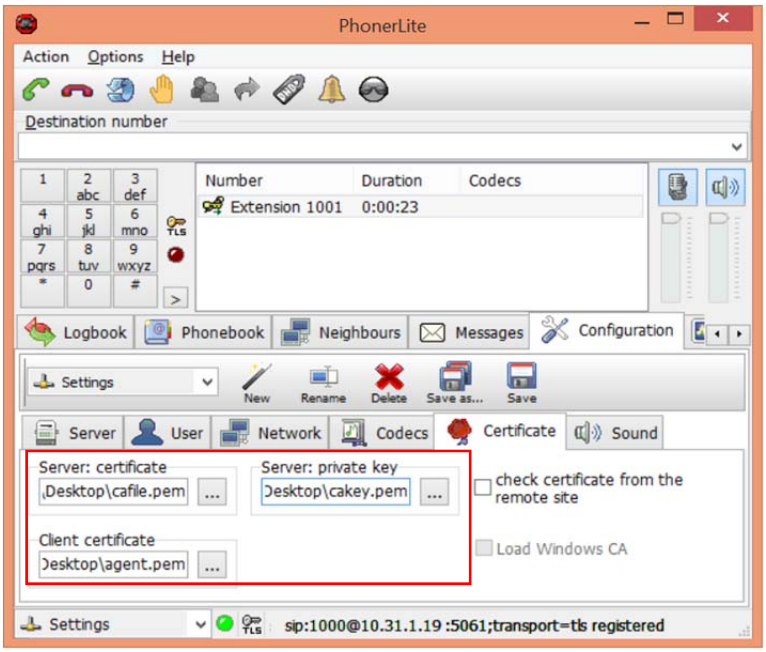
10. จากนั้นไปที่แท็บ Codecs แล้วเลือก SRTP และ SAVP



รูปที่ ค-12 ตั้งค่าใช้งาน SRTP

- เลือกที่ Codec G.711 เลือกที่ SRTP เลือกที่ SAVP กดปุ่ม Save

11. ทำการตั้งค่าใช้งาน SIPS โดยการ



รูปที่ ค-13 ตั้งค่าใช้งาน SRTP

ทำการติดตั้ง Certificate ที่ได้จากระบบ ISANBox.F

ภาคผนวก ง
โปรแกรมตรวจสอบการโจมตี SIP Flooding

โปรแกรมตรวจสอบการโจมตี SIP Flooding

วิทยานิพนธ์นี้ได้ทำการพัฒนาต่อยอดไลบารี่ Jain-SIP เข้าไปต่อยอดในคลาส Proxy โดยเขียนโค๊ดเพิ่มเข้าไปในส่วนของเมธทอด processInvite เพื่อใช้ในการตรวจการโจมตีจากข้อความ Invite ของ SIP Proxy ซึ่งมีรายละเอียดดังนี้

==========

```
int c = 3;
String ar[] = logText.split("\n");//split logtext each line.
int cFlood = 0;
String fTagTMP2 = "";
for (int i = 0; i < ar.length; i++) {//all Message response

		String fTag[] = ar[c].split(";");
		String ip[] = fTag[0].split(":");
		boolean ipBocked = false;

//  1. IP check has been blocked.
		try {
			BufferedReader br2 = new BufferedReader(new FileReader(new File("sipflooding.log ")));
			String line2;
			try {
				while ((line2 = br2.readLine()) != null) {
					String sIP[] = line2.split(" ");
					if (sIP[8].equals(ip[2])) {
						ipBocked = true;
						break;
					}
				}
			} catch (IOException e) {e.printStackTrace();}
		} catch (FileNotFoundException e) {e.printStackTrace();}

		if(ipBocked == false) {
			if (fTagTMP2.equals(fTag[0])){
				cFlood ++;

//2. Check same  IP more than 10 time
				if (cFlood > 10) {

//3. Update Iptables rule

					String UserAdmin = "administrator";
					String passAdmin = "...";
					String cmdBlock = "iptables -A INPUT -i eth1 -s "+ip[2]+" -j DROP";

					try {
						Process p = Runtime.getRuntime().exec(cmdBlock);
						Process p3 = Runtime.getRuntime().exec("service iptables reload");

						p.waitFor();
						ipBocked = true;

//4. Write attack detail to log file sipflooding.log.

						FileWriter writer = new FileWriter(new File("sipflooding.log"), true);
```

```
                                                    DateFormat dateFormat = new SimpleDateFormat("yyyy/MM/dd
                                                    HH:mm:ss");
                                                    Date date = new Date();
                                                    String dt = dateFormat.format(date)+"SIP Flooding From Source IP
                                                    :"+ip[2];
                                                    writer.write(dt+"\n");
                                                    writer.flush();

//5. Post to VoIP Admin Team Facebook Group

                                                    if(Desktop.isDesktopSupported()){
                                                        Desktop.getDesktop().browse(new
                                                        URI("https://www.isan.msu.ac.th/prdit/fb/index.php?ip="+ ip[2]));
                                                    }
                                                    break;
                                                }catch(IOException e1) {}

                                        }//check 10 time
                                        fTagTMP2 = fTag[0];
                }else {
                                cFlood = 0;
                                fTagTMP2 = fTag[0];
                }
}//check Blocked
c+=9;
}//
```

จากตัวอย่างโค๊ดจะมีส่วนการทำงานหลักๆ อยู่ 5 ส่วนดังนี้

1. IP check has been blocked คือส่วนการตรวจสอบว่า IP ที่ส่งข้อความ Invite เข้ามามีการถูกบล็อกอยู่ใน Block list แล้วหรือเปล่า ถ้ามีการบล็อกแล้วจะไม่ทำงานต่อแต่ถ้ายังไม่บล็อกจะเข้าตรวจสอบในขั้นตอนต่อไป

2. Check same IP more than 10 time คือส่วนการตรวจสอบว่าถ้ามีหมายเลขไอพีต้นทางเดิมส่งข้อความ Invite มาซ้ำและติดต่อกันมากกว่า 10 ครั้ง จะดำเนินการในส่วนต่อไป

3. Update Iptables rule คือส่วนการเพิ่มกฎใน Iptables ให้บล็อกไอพีของผู้โจมตี

4. Write attack detail to log file sipflooding.log. คือส่วนการออกรายงานการโจมตีไปไฟล์ sipflooding.log

5. Post to VoIP Admin Team Facebook Group คือส่วนการเรียกใช้ Facebook API ในการแจ้งเตือนการโจมตีไปยังกระดานของเฟสบุ๊คกลุ่ม VoIP Admin Team

ประวัติย่อผู้วิจัย

ประวัติย่อผู้วิจัย

ชื่อ นามสกุล	ร้อยตำรวจโทประดิษฐ์ วงศ์สกุล
วัน เดือน ปีเกิด	วันที่ 20 กรกฎาคม พ.ศ. 2532
จังหวัด และประเทศที่เกิด	อำเภอเมืองมหาสารคาม จังหวัดมหาสารคาม
ประวัติการศึกษา	พ.ศ. 2550 มัธยมศึกษาตอนปลาย โรงเรียนท่าขอนยางพิทยาคม จังหวัดมหาสารคาม
	พ.ศ. 2552 หลักสูตรนักศึกษาวิชาทหารชั้นปีที่ 5 มณฑลทหารบกที่ 23
	พ.ศ. 2554 ปริญญาวิทยาศาสตรบัณฑิต (วท.บ.) สาขาวิชาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยมหาสารคาม
	พ.ศ. 2557 หลักสูตรการฝึกอบรมข้าราชการตำรวจ และบุคคลที่บรรจุหรือโอนมาเป็นข้าราชการตำรวจชั้นสัญญาบัตร (กอส. รุ่นที่ 36) โรงเรียนนายร้อยตำรวจ
	พ.ศ. 2558 ปริญญาวิทยาศาสตรมหาบัณฑิต (วท.ม.) สาขาวิชาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยมหาสารคาม
ตำแหน่ง สถานที่ทำงาน	รองสารวัตร กลุ่มงานเทคโนโลยีสารสนเทศ บก.อก. ตำรวจภูธรภาค 4
ที่อยู่ที่สามารถติดต่อได้	ที่อยู่ 64 หมู่ที่ 2 ตำบลขามเรียง อำเภอกันทรวิชัย จังหวัดมหาสารคาม 44100

ทุนวิจัยและทุนการศึกษา

โครงการทุนพัฒนาศักยภาพทางการวิจัย ประจำปีการศึกษา 2555

ผลงานวิจัย

[1] ประดิษฐ์ วงศ์สกุล, สมนึก พ่วงพรพิทักษ์. “การเสริมสร้างความมั่นคงและประเมินคุณภาพการให้บริการของไอสานบ๊อกด็อทเอฟ”. วารสารวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยมหาสารคาม ฉบับที่ 4 ปีที่ 34 ISSN: 1686-9664

[2] Pradit Wongsakul, Somnuk Puangpronpitag. "Quality of Service Evaluation for VoIP Open Source Software Asterisk VS. FreeSWITCH VS. Kamailo in Real Network", In Proceedings of The National Conference on Information Technology: (NCIT 2013), Petchaburi, Thailand, 26-27 February 2013, pp. 119-124. (in Thai)

[3] Pradit Wongsakul, Piyanat Suyangkul, Somnuk Puangpronpitag. "A Secure Voiceover Internet Protocol (VoIP) System by Extending FreeSWITCH", In Proceedings of The National Conference on Computer Information Technologies (CIT), Chiangmai, Thailand, 13 Feb 2012, pp. 168-173. (in Thai)