การเสริมสร้างความมั่นคงและประเมินคุณภาพการให้บริกาของไอสานบ๊อกด็อทเอฟ
The Security Enhancement and Voice Quality Evaluation of ISANBox.F

ประดิษฐ์ วงศ์สกุล[1], สมนึก พ่วงพรพิทักษ์[2]
Pradit Wongsaku[1], Somnuk Puangpronpitag[2]
Received: 10 September 2014 ; Accepted: 26 December 2014

บทคัดย่อ
ชุดซอต์แวร์เสรี “ฟรีสวิตช์” เป็นซอฟต์แวร์ที่มีประสิทธิภาพสูงทั้งด้านการรองรับคู่สายได้จำนวนมาก มีเสถียรภาพในการทำงาน มีฟังก์ชันการใช้งานพื้นฐานและมีคุณภาพการให้บริการที่ดี แต่ก็ยังพบความเสี่ยงที่จะเกิดปัญหาทางด้านความมั่นคงปลอดภัย เช่น การโจมตี SIP Session Hijacking การโจมตี SIP Flooding การการโจมตี Cancle/bye Attack การโจมตีดักฟังเสียง (RTP Sniffing) เนื่องจากงานวิจัยก่อนหน้านี้[9] (ISANBox.F รุ่น 1) ได้พัฒนาระบบ VoIP จากซอฟต์แวร์ FreeSWITCH ที่มีคุณสมบัติเด่นทางด้านความมั่นคง แต่ยังขาดการป้องกันความมั่นคงในระดับ Signaling Protocol ซึ่งจะทำให้คุณสมบัติความมั่นคงยังไม่สมบูรณ์ อีกทั้งยังไม่มีการประเมินคุณภาพการให้บริการของระบบ ดังนั้นงานวิจัยนี้จึงได้เสนอการพัฒนาต่อยอดฟรีสวิตช์เพื่อแก้ไขความไม่สมบูรณ์ของงานวิจัยก่อนหน้าโดยใช้เทคนิค Secure SIP จากนั้นได้ทำการทดสอบประสิทธิภาพด้านความมั่นคงและคุณภาพการให้บริการ (QoS) ซึ่งจากผลการทดสอบแสดงให้เห็นถึงประสิทธิภาพของการพัฒนาต่อยอดทางด้านความมั่นคง คือระบบสามารถป้องกันการโจมตีในระดับ Signaling Protocol ได้ และจากการพัฒนาด้านความมั่นคงส่งผลต่อคุณภาพการให้บริการของระบบเพียงเล็กน้อย และมีคุณภาพการให้บริการในระดับที่ดี เป็นไปตามที่มาตรฐานที่คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) กำหนด

คำสำคัญ : วีโอไอพี คุณภาพการให้บริการของวีโอไอพี RTP Sniffing SIP Flooding ฟรีสวิตช์

Abstract
FreeSWITCH is a highly efficient Voice over IP (VoIP) package that can serve a high number of concurrent calls. It has also been well-known for its reliability, functionality and quality. However, from literature, FreeSWITCH is still vulnerable to security threats, such as SIP Session Hijacking, SIP flooding, Cancel/Bye Attacks, Voice Eavesdropping by sniffing RTP. In the previous work (ISANBox.F version 1), we developed a VoIP package by extending the security option in FreeSWITCH. Yet, it is still lacking in the security of the signaling protocol. Furthermore, the quality of voices after security enhancement has not yet been evaluated. Hence, in this paper, we propose to extend Free SWITCH to protect against the aforementioned security threats. Furthermore, this research has also developed the GUI and installation set to increase user-friendliness of FreeSWITCH. At the end, we have experimented on our extended FreeSWITCH to investigate both security and quality issues. The experimental results has demonstrated that the extended package is more secure. Also, the security overhead from our implementation have minimal effects on its quality. By using MOS and R-factor as quality metrics, we have found that our extended package still fits very well with the VoIP quality standard of the National Broadcasting and Telecommunication Commission (NBTC).

Keyword : VoIP, VoIP Quality of Service, RTP Sniffing, SIP Flooding, FreeSWITCH

---

[1] *นิสิตหลักสูตรมหาบัณฑิต, [2]อาจารย์, สาขาวิทยาการคอมพิวเตอร์ คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม จังหวัดมหาสารคาม 44150 ประเทศไทย*

[1] *Master degree student, [2]Lecturer Computer science major, Faculty of Informatics, Mahasarakham University, MahaSarakham 44150 Thailand*

บทนำ

ปัจจุบันเทคโนโลยี Voice over Internet Protocol (VoIP) เริ่มเป็นที่นิยมนำมาประยุกต์ใช้งานในหน่วยงานทั้งภาครัฐและเอกชน เนื่องจากเป็นวิธีที่ช่วยลดต้นทุนค่าโทรศัพท์ให้กับองค์กรเป็นอย่างมาก โดยที่เทคโนโลยี VoIP จะทำงานผ่านโครงสร้างพื้นฐานของระบบอินเทอร์เน็ต จึงไม่ต้องลงทุนซื้ออุปกรณ์เพิ่ม ซึ่งทางคณะกรรมการกิจการโทรคมนาคมแห่งชาติ (กทช.)[1] ก็ได้ออกประกาศแนะนำให้ใช้บริการเทคโนโลยี VoIP

ซอฟต์แวร์ในกลุ่ม VoIP Open-source ก็กำลังเป็นที่นิยมเพราะไม่มีค่าใช้จ่ายในการติดตั้งใช้งาน เนื่องจากมีความยืดหยุ่นในการปรับแต่งสูง ง่ายต่อการจัดการ เช่น Asterisk[2], FreeSWITCH[3], Kamailo[4] ซึ่งในส่วนของ VoIP Open source Software ก็มีฟังก์ชันด้านความมั่นคง เช่น ซอฟต์แวร์ FreeSWITCH ตั้งแต่รุ่น 1.0.6 เป็นต้นมาก็มีฟังก์ชันทางด้านความมั่นคง เช่น ฟังก์ชัน Secure SIP (SIPS)[5] ที่ป้องกันการโจมตีระดับสัญญาณ ฟังก์ชัน Secure Reatime Transport Protocol (SRTP)[6] ที่ใช้ในการเข้ารหัสและส่งข้อมูลเสียง อีกทั้ง FreeSWITCH ยังมียังมีคุณสมบัติโดดเด่นกว่าซอฟต์แวร์เสรีอื่นในการรองรับคู่สายได้จำนวนมากและเรื่องความเสถียรในการใช้งานอีกด้วย

มีงานวิจัยที่แสดงให้เห็นถึงปัญหาด้านความมั่นคงของ VoIP ในระดับ Signaling Protocol[7] และปัญหาด้านความมั่นคงของซอฟต์แวร์ VoIP ได้แก่ Asterisk FreeSWITCH และ OpenSER คือทั้ง 3 ซอฟต์แวร์ถูกโจมตีด้วยวิธีการ Man in The Middle Attack (MiTM) วิธี SIP Register Hijacking และ SIP Flooding ได้โดยง่าย[8]

ในงานวิจัยก่อนหน้านี้ร่วมกับปิยะณัฐ สุยังกุล[9] ได้นำเอาซอฟต์แวร์ FreeSWITCH รุ่น 1.0.6 มาพัฒนาต่อยอดเพื่อแก้ไขปัญหาดักฟังเสียงได้สำเร็จ แต่ก็ยังเหลือปัญหาด้านความมั่นคงที่ยังไม่สามารถป้องกันความมั่นคงในส่วนของ Signaling Protocol ได้ อีกทั้งหลังจากที่แก้ไขปัญหาด้านความมั่นคงแล้วก็ยังไม่มีการประเมินคุณภาพการให้บริการว่าเป็นไปตามมาตรฐานหรือข้อกำหนดหรือไม่

ด้วยเหตุนี้งานวิจัยนี้จึงได้เสนอพัฒนาต่อยอด โดยนำเอา FreeSWITCH รุ่น 1.2.6 มาปรับแต่งประยุกต์ใช้ SIPS เพื่อรักษาความมั่นคงของ Signaling Protocol และใช้การส่งข้อมูลแบบ SRTP เพื่อเข้ารหัสข้อมูลเสียง แก้ไขปัญหาการดักฟังเสียงสนทนา จัดการไฟล์ล็อกเพื่อป้องกันการโจมตีแบบ SIP Flooding และพัฒนา User Interface ที่สนับสนุนภาษาไทย พัฒนาแผ่นติดตั้งแบบอัตโนมัติให้สะดวกต่อการติดตั้ง อีกทั้งยังได้ทำการประเมินคุณภาพการให้บริการเพื่อให้ได้สารสนเทศที่ถูกต้องและเป็นประโยชน์ไปใช้ในการวางแผนปรับปรุงให้เครือข่าย VoIP มีคุณภาพการให้บริการที่ดีที่สุด

1. FreeSWITCH

FreeSWITCH[3] คือ ซอฟต์แวร์ที่ถูกพัฒนาขึ้นในปี ค.ศ. 2006 จากทีมผู้สร้าง Asterisk เดิมโดยการนำของ Anthony Minessale โดยเน้นแก้ปัญหาเรื่องประสิทธิภาพการใช้งานของ FreeSWITCH ทำหน้าที่เป็น IP-PBX ในปัจจุบันยังมีการพัฒนาฟังก์ชันทำงานได้หลากหลายเท่า Asterisk แต่เนื่องด้วยการออกแบบที่ใช้โครงสร้าง XML ไฟล์ได้ดีกว่า Asterisk[10-11] ทำให้รองรับการทำงานใช้คู่สาย ณ เวลาเดียวกัน (Concurrent Call) ได้มากกว่า Asterisk ระบบมีความเสถียรมากกว่า Asterisk และยังรองรับมาตรฐานของ Signalling Protocol ได้ดีกว่า Asterisk เนื่องจาก FreeSWITCH ได้ถูกพัฒนาจาก SIP-Sofia[12] ซึ่งเป็นไลบรารีสำหรับพัฒนาซอฟต์แวร์ VoIP ที่เป็นไปตามมาตรฐานโพรโทคอล SIP และมีการใช้ SQLlite เพื่อเก็บค่า Configure ของระบบ และที่น่าสนใจคือมีฟังก์ชันด้านความมั่นคง เช่น สนับสนุนการทำงานของโพรโทคอล SIPS และ SRTP เป็นต้น

2. Secure Realtime Transport Protocol (SRTP)

SRTP[6] เป็นโพรโทคอลที่ถูกออกแบบและพัฒนามาเพื่อเข้ารหัสข้อมูล แก้ไขปัญหาการดักฟังข้อมูลเสียงของโพรโทคอล RTP[13] ถูกใช้ในการส่งข้อมูลมัลติมีเดีย ซึ่งจะทำงานโดยเข้ารหัสและรับรองความถูกต้องของข้อมูล โดยมีการนำมาประยุกต์ใช้ใน VoIP เพื่อเข้ารหัสข้อมูลเสียงก่อนส่งข้อมูลเข้าไปในเครือข่าย ช่วยรักษาความลับระหว่างการติดต่อสื่อสารโพรโทคอล SRTP จะทำงานได้อย่างมีประสิทธิภาพทั้งในเครือข่ายแบบมีสายและไร้สาย SRTP เป็นโพรโทคอลทางด้านความมั่นคงที่ทำงานอยู่ระหว่าง Application Layer และ Transport Layer โดยผู้ส่งจะมีการสร้างแพ็กเกต SRTP แล้วส่งต่อแพ็กเกตนี้ไป ถึงผู้รับในทำนองเดียวกันผู้รับก็ต้องถอดรหัสแพ็กเกต SRTP เพื่อรับฟังข้อมูลเสียงจากผู้ส่ง ซึ่งการเข้ารหัสข้อมูล SRTP มีการเข้ารหัสและใช้หลักการ Session Key มีวิธีการแลกเปลี่ยนกุญแจในการเข้าและถอดรหัสหลายรูปแบบซึ่งขึ้นอยู่กับลักษณะการใช้งานที่ต้องการ

3. Secure SIP (SIPS)

SIPS[5] ถูกออกแบบและพัฒนามาเพื่อเข้ารหัสรักษาความลับของ SIP Session สำหรับ VoIP โดยใช้หลักการทำงานของ Transport Layer Security (TLS)[14] ซึ่งเป็นโพรโทคอลที่ใช้เข้ารหัส รักษาความลับ ใช้ส่งข้อมูลบนเครือข่ายอินเทอร์เน็ตโดยอาศัย Certificate Authority (CA)[15] เช่น เว็บเพจ อีเมล์ เป็นต้น SIPS ถูกพัฒนาเข้ากับซอฟต์แวร์วีโอ

ไอพี ให้เป็นฟังก์ชันด้านความมั่นคง โดยฟังก์ชัน SIPS นี้ได้ถูกพัฒนาขึ้นในฟรีสวิตช์ตั้งแต่รุ่น 1.0.6 เป็นต้นมา ซึ่งถ้าหากมีการติดตั้งและเปิดใช้งานฟังก์ชัน SIPS ก็จะทำให้ VOIP สามารถป้องกัน การโจมตี SIP Session ไม่ให้ถูกดักจับข้อความ SIP Register เพื่อค้นหา User และ Password ของหัวโทรศัพท์ และป้องกันการโจมตีแบบ Cancel/Bye Attack ได้

4. ความมั่นคงและการโจมตีระบบ VoIP

จากศึกษางานวิจัยทางด้านความมั่นคงของระบบ VoIP[7-8, 16-18] พบว่ามีการเสนอช่องโหว่ด้านความมั่นคงและรูปแบบการโจมตีที่หลากหลาย ทั้งในระดับ Media Protocol และ Signalling Protocol ซึ่งการโจมตีในแต่ละระดับก็จะส่งผลกับระบบที่แตกต่างกันออกไป ซึ่งงานวิจัยนี้ได้ให้ความสำคัญและมุ่งต่อยอดแก้ไขปัญหาการโจมตีทั้ง Media Protocol และ Signalling Protocol ดังนี้

1) การโจมตี Signalling Protocol

SIP Register Hijacking โดยปกติ User Agent Client (UAC) ต้องทำการยืนยันตัวตนและบอกตำแหน่งกับ IP-PBX Server ก่อนจึงสามารถใช้งานได้ ถ้าในขณะนั้นหากแฮกเกอร์แทรกแซงการสื่อสาร และแก้ไข Contact field ของข้อความ SIP ให้เปลี่ยนเป็นไอพีแอดเดรสของแฮกเกอร์ ดังนั้นเมื่อมีสายเรียกเข้า (invite) IP-PBX Server จะทำการส่ง packet ไปยังตำแหน่งของแฮกเกอร์จากนั้นแฮกเกอร์พยายามค้นหารหัสผ่านที่ใช้ลงทะเบียนจากข้อความ SIP Register ที่ดักจับได้ด้วยวิธีต่างๆ เช่น Directory Attack, Brute-force attack เป็นต้น

SIP Flooding คือ การโจมตีโดยการส่งข้อความ Invite จากแฮกเกอร์มายัง IP-PBX Server ด้วยอัตราที่เร็วกว่าปกติ ส่งผลให้ IP-PBX Server มีภาระการทำงานมากขึ้น จนทำให้เกิดการปฏิเสธการให้บริการต่อผู้ใช้ทั่วไป โดยปกติวิธี Flooding Attack จะโจมตีมจากต้นทางเดียวจึงเป็นวิธีที่ง่ายต่อการตรวจสอบ

Cancel/Bye Attack คือการโจมตีที่แฮกเกอร์พยามยุติการสื่อสารของเหยื่อโดยการปลอมแปลง SIP Message ให้เป็น CANCEL หรือ BYE เพื่อยกเลิกและสิ้นสุด Session การสื่อสาร ทำให้การสื่อสารนั้นสิ้นสุดลง

2) การโจมตี Media Protocol

RTP Sniffing คือการโจมตีที่แฮกเกอร์แทรกกลางการสื่อสารแล้วดักจับ RTP Streaming เพื่อดักฟังการสนทนาสื่อสาร ซึ่งหากการโจมตีนี้เกิดขึ้นกับองค์กรที่มีการสื่อสารผ่าน VoIP เช่น ข้อมูลทางธุรกิจ เลขบัญชีหรือข้อมูลความลับของสินค้า หรือรหัสผ่าน ถ้าข้อมูลดังกล่าวรั่วไหลไปก็จะเกิดความเสียหายที่ร้ายแรงต่อองค์กรที่ใช้ระบบ VoIP ได้ ดังนั้นปัญาการโจมตีในระดับ Media Protocol โดยเฉพาะการดักฟังเสียงสนทนานี้จึงเป็นประเด็นที่งานวิจัยได้ให้ความสำคัญที่จะแก้ไขปัญหา

5. งานวิจัยที่พัฒนาปรับปรุงซอต์ฟแวร์ FreeSWICTH

ISANBox.F V.1[9] คืองานวิจัยที่มุ่งพัฒนาต่อยอดฟรีสวิตช์ โดยได้แก้ปัญหาด้านความมั่นคงในระดับ Media Protocol เป็นหลักคือ แก้ปัญหาการดักฟังเสียง และแก้ไขปัญหาการโจมตี SIP Flooding งานวิจัยยังได้เสนอการพัฒนา Web User Interface และส่วนการติดตั้งทำให้ผู้ใช้เกิดความสะดวกใช้งานง่าย ซึ่งงานวิจัยนี้ยังคงพบปัญหาในระดับ Signalling Protocol เช่น การโจมตี SIP Session Hijacking การโจมตี SIP Flooding การการโจมตี Cancle/bye Attack การโจมตีดักฟังเสียง (RTPSniffing) ที่ยังไม่ถูกแก้ปัญหา อีกทั้งยังไม่ได้มีการทดสอบคุณภาพการให้บริการว่าเป็นไปตามที่มาตรฐาน กำหนดหรือไม่

BuleBox[19] คืองานวิจัยที่การพัฒนาส่วนติดต่อผู้ใช้งาน (Graphic User Interface) และส่วนการติดตั้งที่เน้นความสะดวกสบาย ใช้งานง่ายต่อทั้งผู้ดูแลระบบและผู้ใช้ทั่วไป สามารถบริหารจัดการปรับแต่งค่าพื้นฐานของระบบผ่านทางหน้าเว็บได้ แต่งานวิจัยนี้ไม่ได้เน้นการพัฒนาด้านความมั่นคงและยังไม่ได้มีการทดสอบคุณภาพการให้บริการเช่นเดียวกันกับ ISAN.F V.1

6. การวัดคุณภาพการให้บริการของ VoIP

จากงานวิจัย[20-23] พบว่าผลการพัฒนาด้านความมั่นคงจะส่งผลกับคุณภาพการให้บริการ ทั้งนี้ก็เกิดจากภาระงานของระบบการประมวลผลที่เพิ่มขึ้น เช่น การคำนวณเข้ารหัสและถอดรหัสข้อมูล ซึ่งมีวิธีการประเมินคุณภาพการให้บริการเป็นที่นิยมหลักๆอยู่ 2 วิธีดังนี้

1) Mean Opinion Score[24] ได้มีการกำหนดให้เป็นมาตรฐานโดย ITU-T P.800 เป็นวิธีการวัดความพอใจของผู้ใช้งาน เป็นการวัดเชิงคุณภาพ (Subjective) โดยจะต้องใช้ผู้ทดลองจำนวนมากเพื่อเพิ่มความน่าเชื่อถือให้มากขึ้น แล้วให้ผู้ฟังแต่ละคนให้คะแนนความพึงพอใจของเสียงที่ได้ยิน ซึ่งจะมีคะแนนเริ่มตั้งแต่ 1 ถึง 5 โดยที่ 5 หมายถึงคุณภาพเสียงดีที่สุด และ 1 หมายถึงคุณภาพเสียงน้อยที่สุดตามลำดับดังที่แสดงใน Table 1 แต่วิธีนี้จะมีความยุ่งยากในการจัดการผู้ใช้ที่มาทดลอง และความพึงพอใจของแต่ละคนก็จะมีความแตกต่างกัน อีกทั้งยังมีต้นทุนค่าใช้จ่ายในการวัดด้วยวิธีนี้ที่สูง

Table 1 MOS Values and Qualities of Voice

MOS	คุณภาพ	ลักษณะเสียง
5	ยอดเยี่ยม	คาดไม่ถึง
4	ดี	ใช้ได้
3	พอใช้	หงุดหงิดเล็กน้อย
2	ไม่ดี	ไม่น่าพอใจ
1	แย่	ไม่พอใจ

2) E-Model เป็นรูปแบบการวัดคุณภาพเสียงที่ถูกกำหนดโดย ITU-T G.107[25] ซึ่งใช้ค่า R Factor (0-100) ในการเปรียบเทียบกับค่า MOS ซึ่งจะครอบคลุมปัจจัยสภาพแวดล้อมต่าง ๆที่มีผลต่อคุณภาพเสียงเช่น Delay Packet Loss และ Jitter และมีข้อดีคือต้นทุนต่ำใช้งานได้สะดวก ซึ่งสามารถคำนวณเปลี่ยนค่า R Factor มาเป็นค่า MOS สามารถคำนวณได้ดังนี้

$$\text{MOS} = \begin{cases} 1 & \text{เมื่อ } R<0 \\ 1+0.035\,R+R(R-60)(100-R)7\times10^{-6} & \text{เมื่อ } 0<R<100 \\ 4.5 & \text{เมื่อ } R>100 \end{cases}$$

ซึ่งสามารถคำนวณค่า R ได้ดังนี้

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

R_0 คือ อัตราส่วนระหว่างสัญญาณต่อเสียงรบกวน (Signal to Noise Ratio)

I_s คือ ค่าบกพร่องทั้งหมดที่เกิดขึ้นมากหรือน้อยที่เกิดขึ้นพร้อมกันกับสัญญาณเสียง

I_d คือ ค่าความบกพร่องที่เกิดจากความล่าช้า (Delay)

$I_{ef\text{-}eff}$ คือ ค่าการสูญเสียของแพ็กเกต (Packet Loss) ที่มี ผลจากความบกพร่องของอุปกรณ์

A คือ ค่าปัจจัยได้เปรียบในการเข้าถึงอุปกรณ์

แต่เนื่องจาก R Factor เป็นการคำนวณค่าปัจจัยของเครือข่าย ซึ่งเป็นสูตรคณิตศาสตร์ที่ซับซ้อน ได้มองว่าการคำนวณที่มีคุณภาพจะถูกกำหนดโดย ค่าความบกพร่องที่เกิดจากความล่าช้า (Delay) และค่าการสูญเสียแพ็กเกต (Packet Loss) ที่มีผลจากความบกพร่องของอุปกรณ์ ซึ่งครอบคลุมการสูญเสียข้อมูลเนื่องจากการเข้ารหัสและการสูญเสียแพ็กเกต (Packet Loss) จึงมีการลดทอนสูตรให้ง่ายต่อการคำนวณค่า R ที่มีคุณภาพดังนี้

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

โดยที่

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

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

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

I_e = Equipment Impairment Factor ค่าตาม Table 2

Bpl = Packet Lost Robustness Factor ค่าตาม Table 2

Table 2 I_e and *Bpl* Values

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

Table 2 แสดงถึงค่า I_e และ *Bpl* ของแต่ละ CODEC โดยงานวิจัยนี้ได้ศึกษาวิจัย Default CODEC ของ FreeSWITCH นั่นคือ G.711 ดังนั้นจึงใช้ ค่า I_e = 0 และ *Bpl* = 4.3 ในการคำนวณ

ซึ่งในประเทศไทย โดยสำนักงานคณะกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (กสทช.)[26] ได้มีข้อกำหนดถึงมาตรฐานคุณภาพเสียงผ่านระบบ VoIP ที่ยอมรับได้ต้องมีค่า MOS 3.6 หรือค่า R Factor เท่ากับ 70 ขึ้นไป

มูลเหตุของงานวิจัย

เนื่องจากงานวิจัยก่อนหน้านี้[9] ได้พัฒนาระบบ VoIP จากซอฟต์แวร์ FreeSWITCH ที่มีคุณสมบัติเด่นทางด้านความมั่นคง โดยป้องกันการดักฟังเสียงและป้องกันการโจมตีแบบ SIP Flooding แต่ยังขาดการป้องกันความมั่นคงในระดับ Signaling Protocol ซึ่งจะทำให้คุณสมบัติความมั่นคงยังไม่สมบูรณ์ อีกทั้งในงานวิจัยก่อนหน้ายังไม่มีการประเมินคุณภาพการให้บริการของระบบ VoIP และในงานวิจัย BlueBox[19] ก็มีจุดเด่นที่ส่วนติดต่อผู้ใช้งานและส่วนการติดตั้งที่สะดวกใช้ง่าย แต่ไม่ได้มีการแก้ปัญหาด้านความมั่นคงและไม่ได้มีการทดสอบคุณภาพการให้บริการแต่อย่างใด

ดังนั้นงานวิจัยนี้จึงได้เสนอการพัฒนาต่อยอดงานวิจัยก่อนหน้าเพื่อป้องกันการโจมตีในระดับ Signaling Protocol และทำการประเมินคุณภาพการให้บริการเพื่อให้ได้สารสนเทศเกี่ยวกับคุณภาพการให้บริการ ที่สามารถใช้ในการวางแผนจัดการระบบ VoIP ให้สอดคล้อง เป็นที่พึงพอใจต่อผู้ใช้งาน โดยได้ตั้งชื่อให้ระบบใหม่ที่พัฒนาต่อยอดนี้ว่า “ISANBox.F V.2” โดยทั้งนี้ถือเป็นการพัฒนาต่อยอดจากทีมวิจัยเดิมที่ได้พัฒนาระบบให้บริการที่ยังไม่สมบูรณ์ไว้

วิธีการทดลองและศึกษาวิจัย

1. การออกแบบระบบ

งานวิจัยได้เสนอระบบที่เน้นออกแบบโดยใช้ Open- source Software ออกแบบและทำการพัฒนาอยู่บนระบบปฏิบัติการ CentOS และใช้ VoIP Software คือ FreeSWITCH รุ่น 1.2.6 ใช้ MySQL เป็นฐานข้อมูล ใช้ Apache เป็น Web Server ใช้โปรแกรม PhonerLite ทำหน้าที่เป็น Client ในการโทรติดต่อสื่อสาร พัฒนาเว็บส่วนติดต่อผู้ใช้งานจากภาษา PHP เพื่อให้เกิดความสะดวกและง่ายต่อการติดตั้งจึงได้พัฒนาแผ่นติดตั้งแบบอัตโนมัติโดยนำเอาแพ็กเกจส่วนที่พัฒนาขึ้นมาใหม่ นำมาสร้างเป็นแผ่นติดตั้งพร้อมคู่มือการใช้งาน

เปิดใช้งานฟังก์ชัน SIPS และเปิดใช้งาน SRTP ประยุกต์ใช้ Iptables ซึ่งเป็นชุดคำสั่งไฟล์วอล์ที่ติดมากับระบบปฏิบัติ CentOS ในการป้องกันการโจมตีแบบ SIP Flooding โดยการวิเคราะห์หาการโจมตีจากไฟล์ล็อกของFreeSWITCH ดังแสดงโครงสร้างการออกแบบระบบใน Figure 1

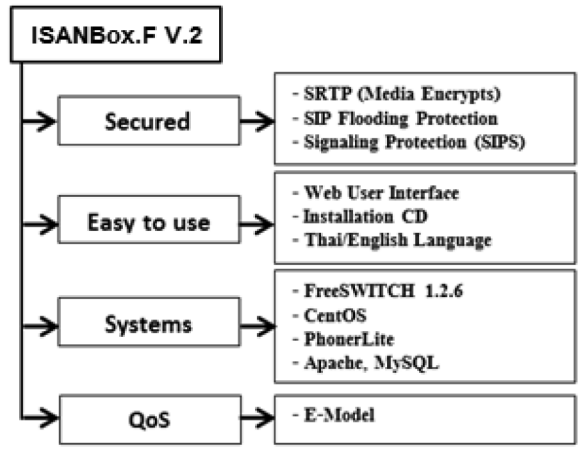

Figure 1 Framework of ISAN Box.F V.2

หลังจากพัฒนาระบบ ISANBox.F V.2 ที่มีความมั่นคงปลอดภัยแล้ว ได้ทำการปะเมินคุณภาพการให้บริการโดยใช้เทคนิค E-Model เพื่อประเมินคุณภาพการให้บริการของระบบ ISANBox.F V.2 ว่ามีคุณภาพการให้บริการอยู่ในระดับที่มาตรฐานกำหนดหรือไม่อย่างไร

การรออกแบบพัฒนา Web User Interface ได้มีการออกแบบแบ่งเป็น 2 ส่วนคือส่วนของผู้ดูแลระบบที่ใช้เพิ่ม ลบ แก้ไข ผู้ใช้งาน อัพโหลดไฟล์ ตรวจสอบการโทร จัดการระบบกับส่วนของผู้ใช้งานที่ใช้จัดการแก้ไขข้อมูลส่วนตัว ดาวน์โหลดเอกสาร โดยระบบจะใช้งานควบคู่กับโปรแกรม PhonerLite รุ่น 2.1 เนื่องจากเป็นโปรแกรมที่รองรับการทำงาน SIPS และ SRTP ซึ่งระบบยังสามารถใช้งานได้กับอุปกรณ์ เช่น เครื่องโทรศัพท์ IP Phone ที่รองรับการทำงานโพรโทคอล SRTP ดังที่แสดงโครงสร้างการทำงานใน Figure 2

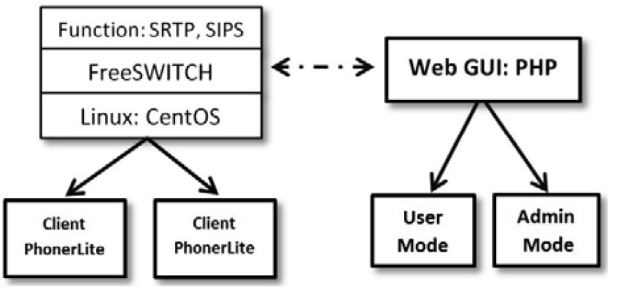

Figure 2 System Structure

เนื่องจากใน FreeSWITCH จะต้องเข้าไปปรับแต่งค่าในไฟล์ XML ที่ยุ่งยาก ดังนั้นใน ISANBox.F V.2 จึงสร้างหน้าเว็บเพื่อใช้ในการเปิด/ปิดใช้งาน SRTP ดังในแสดงใน Figure 3

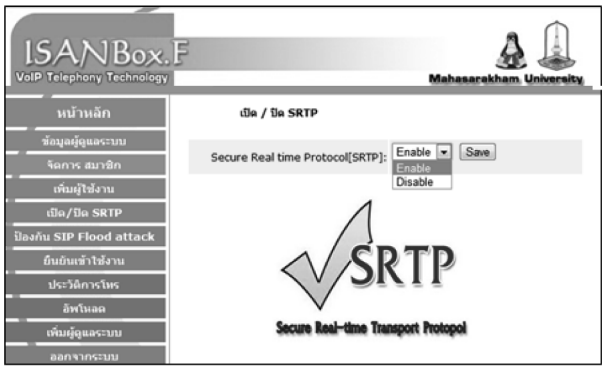

Figure 3 GUI of Disable/Enable module

2. การออกแบบความมั่นคงของระบบ

ในการออกแบบด้านความมั่นคงของระบบได้ทำการเปิดใช้งานฟังก์ชัน SIPS[5] ที่มีในฟรีสวิตช์เพื่อป้องกันการโจมตีในระดับสัญญาณ โดยการติดตั้งแพ็คเกจ libssl-dev เพื่อเปิดใช้งาน OpenSSL ลงบนระบบปฏิบัติการ CentOS จากนั้นทำการสร้าง CA (Root) Certificate ด้วยเรียกใช้ Script ดังนี้

./gentls_certcreate_server -cnisan.msu.ac.th

-alt DNS: isan.msu.ac.th -org isan.msu.ac.th

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

./gentls_cert setup -cnisan.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 สุดท้ายทำการตั้งค่านำเอา Certificate ที่สร้างขึ้นไปตั้งค่าที่ฝั่ง Client ในโปรแกรม PhonerLite ดังแสดงใน Figure 4

Figure 4 Configure Certificate on PhonerLite

ทำการเปิดใช้งานโพรโทคอล SRTP เพื่อเข้ารหัสสัญญาณเสียง ปรับแต่งค่าแท็ก sip_has_crypto อยู่ในไฟล/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/”>

จากนั้นได้พัฒนาระบบป้องกันการโจมตีแบบ SIP Flooding ซึ่งยังไม่มีใน FreeSWITCH โดยทำการตรวจสอบและวิเคราะห์ไฟล์ล็อกของ FreeSWITCH ที่ /usr/local/freeswitch/log/freeswitch.log แล้วทำการเขียนโปรแกรม Batch Shell Script เพื่อตรวจสอบหาการโจมตีในรูปแบบ SIP Flooding เมื่อพบลักษณะไฟล์ล็อกที่เป็นการจู่โจมแบบ SIP Flooding คือทั้ง Invite Flood และ Register Flood ก็ทำการสั่งงาน Iptables ให้เพิ่มกฎเพื่อบล็อกหมายเลขไอพีต้นทางของการจู่โจมที่ตรวจจับได้

3. ประเมินประสิทธิภาพความมั่นคงของระบบ

งานวิจัยได้ทดสอบประสิทธิภาพความมั่นคงของระบบ ISANBox.F V.2 ตามแบบงานวิจัย[27] โดยได้ออกแบบเครือข่ายทดลอง (Test-bed) โดยติดตั้ง ISANBox.F V.2 และใช้โปรแกรม PhonerLite ทำหน้าที่เป็นเครื่อง Client Phone โทรติดต่อสื่อสารกันระหว่าง 2 Client เชื่อมต่อเครือข่ายด้วย Switch L2 โดยมี

เครื่อง Server : Intel i7 4510U CPU 2.6 GHz, 4 GB of RAM, 10/100 Mbps Ethernet Interface Card

เครื่องลูกข่ายทั้ง 2 เครื่อง : ระบบปฏิบัติการ Microsoft Windows 7, Intel(R) Core(TM)2 Duo CPU 2.0 GHz, 2 GB of RAM, 10/100 Mbps Ethernet Interface Card

เครื่องแฮกเกอร์: ระบบปฏิบัติการ Microsoft Windows 7 Intel(R) Core i3 CPU 2.4 GHz, 2 GB of RAM,10/100 Mbps Ethernet Interface Card

จากนั้นทำการวิเคราะห์ปัญหาที่เกิดขึ้นด้วยโปรแกรม Wireshark ดังแผนผังเครือข่ายการทดสอบแสดงใน Figure 5 ซึ่งงานวิจัยได้กำหนดรูปแบบการโจมตีที่สำคัญและมีผลร้ายแรงกับระบบ VoIP ไว้ดังนี้

1) SIP Register Hijacking ด้วยโปรแกรม Cain & Abel โดยโจมตีเพื่อดักจับค้นหาชื่อผู้ใช้และรหัสผ่านของหัวโทรศัพท์ จาก SIP Register Session

2) SIP Flooding โดยใช้ชุดคำสั่ง inviteflood ซึ่งอยู่ใน /pentest/voip ของระบบปฏิบัติการ Backtack 5 เพื่อทำให้ระบบ VoIP เกิดการปฏิเสธการให้บริการต่อผู้ใช้

3) Cancel/Bye Attack ใช้ชุดคำสั่ง teardown ซึ่งอยู่ใน /pentest/voip ของระบบปฏิบัติการ Backtack 5 เพื่อทำการตัดสายโทรศัพท์ ทำให้สิ้นสุดการสื่อสารระหว่างผู้ใช้งาน

4) RTP Sniffing ด้วยโปรแกรม Cain & Abel โดยโจมตีเพื่อดักจับ RTP Streaming แล้วฟังเสียงการสนทนาของผู้ใช้งาน

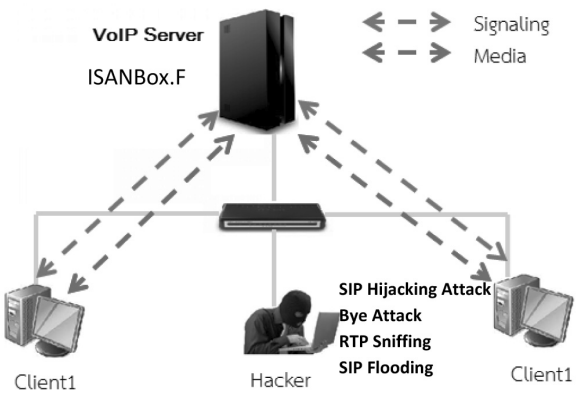

Figure 5 Scenario of security evaluation

4. ประเมินคุณภาพการให้บริการ ISANBox.F V.2

ในการทดสอบวัดค่าคุณภาพการให้บริการได้ออกแบบเครือข่ายทดลองตามแบบในงานวิจัยก่อนหน้า[20]โดยใช้ซอฟต์แวร์ Commview[27] ซึ่งเป็นซอฟต์แวร์ที่ใช้วิเคราะห์ระบบเครือข่าย VoIP ได้ทั้งเครือข่ายแบบสายและไร้สาย โดยเฉพาะฟังก์ชันในการวิเคราะห์ข้อมูลคุณภาพการให้บริการของ VoIP ซอฟต์แวร์นี้สามารถคำนวณค่าคุณภาพการให้บริการ R Factor และค่า MOS จากปัจจัยของเครือข่ายค่า Packet loss ค่า Delay และ jitter ตามแบบการคำนวณของ E-Model ได้อย่างสมบูรณ์

โดยได้ออกแบบติดตั้งเครื่องให้บริการ SIP Server ไว้ใช้เครื่องรับบริการ 30 เครื่อง (Soft phone Clients) เชื่อมต่อผ่านอุปกรณ์เครือข่าย Switch L2 จากนั้นติดตั้งโปรแกรม PhonerLite เป็น Soft phone และ CommView เพื่อใช้ในการวัดค่า MOS และ ค่า R-Factor จากนั้นทำการโทรติดต่อสื่อสารกันระหว่าง Client 30 เครื่องหรือ 15 คู่สายพร้อมกัน (Concurrent Call) จำนวน 30 ครั้ง ใช้เวลาโทรครั้งละ 1 นาที โดยใช้งานโพรโทคอล RTP และ SRTP ในการทดลอง และได้เลือกใช้ CODEC G.711 เพราะเป็น CODEC และเป็นที่นิยมใช้ใน VoIP Software ทั่วไป อีกทั้งยังเป็น Default CODEC ของ FreeSWITCH ใช้ชุดข้อมูลเสียงดนตรีเป็นไฟล์เสียงเดียวกันโดยตั้งค่าให้เล่นไฟล์เสียงแล้วส่งเป็นช่องสัญญาณเข้าไมค์ของโปรแกรม PhonerLite ดังแสดงตัวอย่างเครือข่ายทดลองใน Figure 6

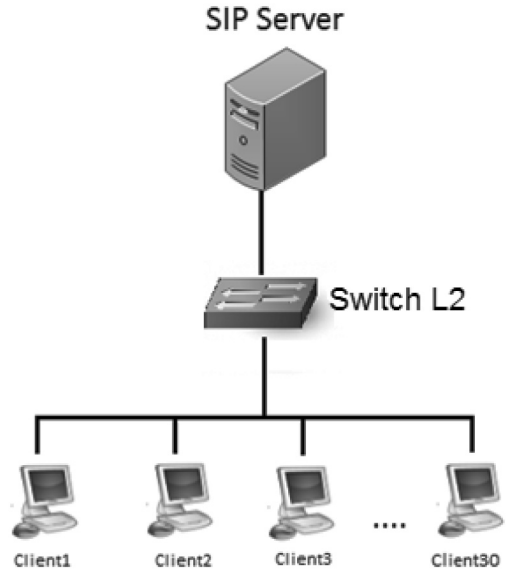

Figure 6 Scenario of QoS Evaluation

แต่การออกแบบเครือข่ายการทดสอบเครือข่ายจริงอาจจะมีปัญหาเรื่องของความหนาแน่นของทราฟฟิกที่ไม่คงที่ อาจจะเกิดความคับคั่งของแพ็กเกตอื่นๆที่ไม่เกี่ยวข้อง ดังนั้นจึงได้ควบคุมปัจจัยที่จะส่งผลต่อการทดลองดังกล่าว โดยการบีบขนาดของ Bandwidth ที่ขาเชื่อมต่อ VoIP Server โดยใช้แพ็กเกต Traffic Control (TC) ที่ถูกติดตั้งมาพร้อมกับ CentOS ในการควบคุมให้ได้ Bandwidth 3 Mbps, 5 Mbps, 10 Mbps และ 100 Mbps และเพื่อเป็นการจำลองบริบทของเครือข่ายที่มีข้อจำกัดทาง Bandwidth ที่แตกต่างกันว่าจะส่งผลต่อคุณภาพการให้บริการระบบวีโอไอพีอย่างไร ซึ่งงานวิจัยใช้หลักการทางสถิติในการเก็บข้อมูลของผลการทดลองและวิเคราะห์ข้อมูล โดยใช้ค่าเฉลี่ย ($\overline{X}$) ของค่า MOS ที่ช่วงความเชื่อมั่น 95 % ในการนำเสนอข้อมูลผลการทดลอง

เพื่อทำการตรวจสอบการติดต่อสื่อสาร อาจจำเป็นต้องบันทึกการสนทนาหรือเก็บประวัติการสนทนา หรืออาจต้องการใช้ระบบฝากข้อความ ดังนั้นการทดลองจึงได้กำหนดค่าบน VoIP Server กำหนดตั้งค่าให้ข้อมูลเสียง (RTP/SRTP Streaming) วิ่งผ่าน VoIP Server โดยที่ข้อมูลจะถูกส่งผ่าน VoIP Server โดยที่ Media Proxy จะมีการสร้างเซสชั่นในการติดต่อสื่อสารโดยใช้โพรโทคอล SIP ส่ง SIP Messages โต้ตอบกันเมื่อสร้างเซสชั่น สำเร็จจึงเริ่มส่งข้อมูลด้วยโพรโทคอล RTP และ SRTP ระหว่าง Client โดยผ่าน VoIP Server ดังแสดงใน Figure 7

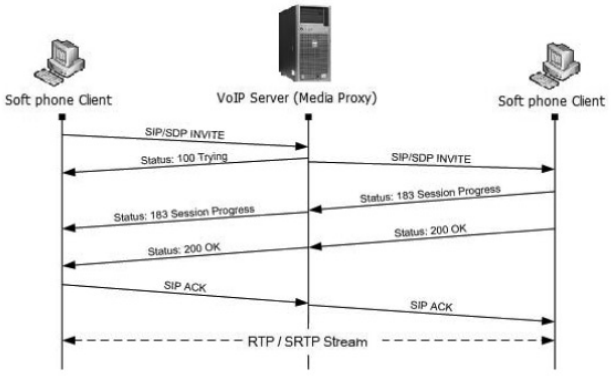

Figure 7 Media Proxy Call Mode

ผลการดำเนินงาน

1. ผลการพัฒนาระบบ

จากงานวิจัยทำให้ได้ระบบ VoIP ที่มีส่วน Web User Interface ที่ใช้งานง่าย อีกทั้งยังมีคุณสมบัติทางด้านความมั่นคง ได้ระบบที่มีคุณภาพการให้บริการเป็นไปตามมาตรฐานที่ กสทช. กำหนด ได้พัฒนาแผ่นติดตั้งแบบอัตโนมัติสะดวกในการติดตั้งใช้งานพร้อมคู่มือที่ชัดเจน ดังแสดงตัวอย่างการติดตั้งใน Figure 8

Figure 8 Installation Module

งานวิจัยได้พัฒนา Web User Interface ที่มีความสะดวก ใช้งานง่ายสนับสนุนภาษาไทย สามารถจัดการเพิ่ม ลบ แก้ไข ผู้ใช้งานระบบ VoIP ได้ผ่านทางหน้าเว็บดังอย่าง Web User Interface ใน Figure 9

Figure 9 Web User Interface

2. ผลการทดสอบทางด้านความมั่นคง

งานวิจัยได้ทดสอบประสิทธิภาพด้านความมั่นคงของ ISANBox.F V.2 และได้ผลการทดสอบประสิทธิภาพดังนี้

1) SIP Register Hijacking ด้วยโปรแกรม Cain & Abel โจมตีเพื่อดักจับค้นหาชื่อผู้ใช้และรหัสผ่านของหัวโทรศัพท์ จาก SIP Register Session ผลปรากฏว่า ไม่สามารถดักจับ User และ Password ผู้ใช้ ของระบบ ISANBox.F V.2 ได้

2) SIP Flooding โดยใช้ชุดคำสั่ง Invite ในBacktack 5 เพื่อทำให้ระบบ VoIP เกิดการปฏิเสธการให้บริการต่อผู้ใช้ ปรากฏว่าไม่เกิดการปฏิเสธการให้บริการของระบบ ISANBox.F V.2 เนื่องจากมี Script ที่ใช้วิเคราะห์และตรวจสอบล็อกไฟล์แล้วสั่ง IP Tables ให้บล็อกไอพีต้นทางของการ Flood

3) Cancel/Bye Attack โดยใช้ชุดคำสั่ง tear-down ใน Backtack 5 เพื่อทำการตัดสายโทรศัพท์ สิ้นสุดการสื่อสารของผู้ใช้งาน ผลปรากฏว่าไม่ส่งผลใดต่อระบบ ISANBox.F V.2 เนื่องจากช่องสัญญาณ SIP จะถูกเข้ารหัสป้องกันด้วย TLS

4) RTP Sniffing ด้วยโปรแกรม Cain & Abel โดยโจมตีเพื่อดักจับ RTP Streaming แล้วฟังเสียงการสนทนาของผู้ใช้งาน ผลปรากฏว่าระบบ ISANBox.F V.2 จะถูกดักจับข้อมูลเสียงได้ แต่เสียงที่ได้จะมีลักษณะที่มนุษย์ฟังไม่รู้เรื่องเนื่องจากถูกเข้ารหัสโดยโพรโทคอล SRTP

เมื่อใช้โปรแกรม Wireshark จับกราฟการไหลของแพ็กเกต พบว่าก่อนการใช้งาน SRTP จะสามารถดักฟังเสียงได้และมีแพ็กเกตดัง Figure 10 ฝั่งซ้าย และหลังใช้งาน SRTP จะฟังเสียงที่ดักมาได้ไม่รู้เรื่องเพราะข้อมูลเสียงจะถูกเข้ารหัสไว้ ดังใน Figure 10 ฝั่งขวา

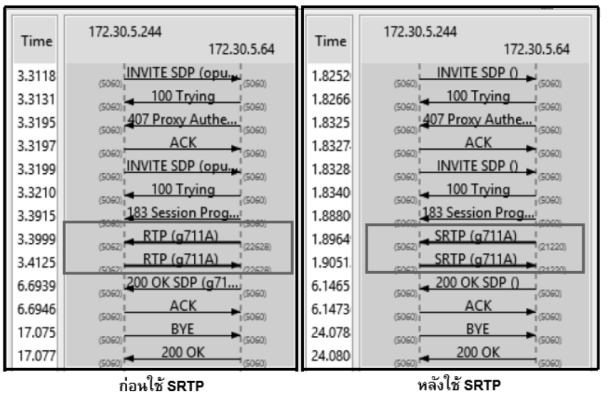

Figure 10 Flow of RTP/SRTP Packet

3. ผลประเมินคุณภาพการให้บริการ

จากการประเมินคุณภาพการให้บริการของ ISANBox.F V.2 และ FreeSWITCH รุ่น 1.2.6 โดยใช้เทคนิควิธี E-Model ภายใต้ข้อจำกัด Bandwidth ที่ต่างกันซึ่งได้ผลคือมีค่า MOS อยู่ในระดับที่ดี นั่นหมายถึงผู้ใช้งานจะมีความพึงพอใจต่อคุณภาพเสียงที่ได้ยินคือมีลักษณะเสียงที่ดีใช้ได้ เสียงไม่ขาดหาย ผู้ใช้มีความรู้สึกพอใจกับคุณภาพเสียง และเป็นไปตามมาตรฐานที่ กสทช. กำหนดไว้ คือค่า MOS 3.6 ขึ้นไป ดังแสดงรายละเอียดค่า MOS ของระบบ ISANBox.F ใน Table 4

Table 4 Quality of Service Evaluation of ISANBox.F V.2 and FreeSWITCH 1.2.6 (MOS Score)

Bandwidth	ค่าเฉลี่ย Mean Opinion Score (MOS)	
	ISANBox.F V.2	FreeSWITCH 1.2.6
3 Mbps	2.15 ± 0.06	2.51 ± 0.06
5 Mbps	2.83 ± 0.05	3.01 ± 0.09
10 Mbps	4.27 ± 0.04	4.31 ± 0.07
100 Mbps	4.32 ± 0.07	4.35 ± 0.02

Table 4 ได้แสดงผลการทดลองเป็นค่าเฉลี่ย ($\overline{X}$) ของค่า MOS ที่ช่วงความเชื่อมั่น 95 % ของ ISANBox.F V.2 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 2.51 ± 0.06 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 V.2 เพราะเป็นผลจากการเข้ารหัสจึงทำให้คุณภาพการให้บริการต่ำลง ซึ่งสอดคล้องกับงานวิจัย[22-25] และใน Bandwidth 10 Mbps และ 100 Mbps จะมีค่า MOS มากกว่า 4 ซึ่งอยู่ในระดับความพึงพอใจที่ดีต่อผู้ใช้งาน และเมื่อลดขนาด Bandwidth ลงมาที่ 5 Mbps และ 3 Mbps พบว่าค่า MOS ของทั้ง 2 ก็ลดลงมาเรื่อยๆ ดังนั้นจากผลการทดลองจึงบอกได้ว่าคุณภาพการให้บริการของ ISANBox.F V.2 ในเครือข่ายทดลองนั้นมีค่า MOS ลดลงต่ำกว่า FreeSWITCH รุ่น 1.2.6 เพียงเล็กน้อยจึงทำให้ไม่ส่งผลต่อคุณภาพการให้บริการของ ISANBox.F V.2 ในระดับที่ผู้ใช้ไม่พึงพอใจ ซึ่งงานวิจัยนี้ได้พบประเด็นที่ผู้ดูแลระบบต้องให้ความสำคัญและคำนึงถึงเพื่อให้ได้ระบบ VoIP ที่มีคุณภาพการให้บริการที่ดีเยี่ยม นั่นคือเรื่องของ Bandwidth ของเครือข่ายที่เหมาะสมกับการใช้งานขององค์กร

เปรียบเทียบคุณสมบัติ ISANBox.F V.2 กับ Blue-box

สืบเนื่องจากซอฟต์แวร์ FreeSWITCH มีการพัฒนาเปลี่ยนผ่านรุ่นอยู่เป็นระยะ ซึ่งในปัจจุบัน (กุมภาพันธ์ พ.ศ. 2558) FreeSWITCH ได้มีการสนับสนุนให้ใช้ส่วนติดต่อผู้ใช้งาน (Grapic User Interface) ซึ่งพัฒนาให้ผู้ใช้ใช้งานได้อย่างสะดวกสะบายในชื่อ Blue Box Project[25] มีการพัฒนามาจนถึง BlueBox รุ่น 1.0.3 โดยงานวิจัยก็ได้ทดลองติดตั้งใช้งานตามค่าเริ่มต้นของระบบ ศึกษาการทำงานและฟังก์ชันต่างๆของ BlueBox จึงได้ทำการเปรียบเทียบถึงคุณสมบัติระหว่าง ISANBox.F V.2 กับ BlueBox ได้ผลดังแสดงใน Table 3

Table 3 Compare Feature of ISANBox.F V.2 and BlueBox

Feature	ISANBox.F V.2	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

จาก Table 3 พบว่าคุณสมบัติหลักๆ ที่ BlueBox ได้พัฒนาคือมุ่งเน้นที่ความสะดวกสบาย สวยงาม และส่วนติดตั้งใช้งานง่าย ส่วนด้านความมั่นคงก็ยังไม่ป้องกันการโจมตีในแบบ SIP Flooding และการโจมตีแบบอื่นๆก็ยังป้องกันไม่ได้ เนื่องจากยังไม่มีการแนะนำและเปิดใช้งานฟังก์ชันด้านความมั่นคงที่ชัดเจนซึ่ง BlueBox ไม่ได้ถูกพัฒนามาเพื่อแก้ปัญหาด้านความมั่นคง

ซึ่งต่างจาก ISANBox.F V.2 ที่งานวิจัยนี้ได้เสนอการพัฒนาเพื่อเพิ่มประสิทธิภาพทางด้านความมั่นคงของระบบเป็นหลักและยังมีส่วนของ User Interface และส่วนการติดตั้งที่ใช้งานง่ายอีกด้วย ดังแสดงภาพ User Interface ของระบบ ISANBox.F V.2 ดังใน Figure 9 และตัวอย่าง User Interface ของ BlueBox ดังใน Figure 11

Figure 11 Web User Interface Bluebox

สรุปผลการศึกษา

จากการพัฒนาระบบ ISANBox.F V.2 ทำให้ได้ระบบที่มีความสามารถในการป้องกันการโจมตี SIP Register Hijacking ป้องกันการโจมตี Cancel/Bye Attack แก้ไขปัญหาการดักฟังเสียงการสนทนา (RTP Sniffing) และป้องกันการจู่โจมแบบ SIP Flooding ซึ่งจะทำให้เกิดผลดีกับองค์กรในด้านการรักษาความลับของข้อมูลเสียงและความมั่นคงของระบบ ISANBox.F V.2 ยังได้ระบบที่มีคุณภาพการให้บริการในระดับที่ดี ผู้ใช้งานพึงพอใจ มีระบบที่ติดตั้งและใช้งานง่ายรวดเร็ว มี Web User Interface ที่สนับสนุนภาษาไทย อีกทั้งยังเป็นผลดีกับเศรษฐกิจองค์รวมของประเทศเพราะไม่ต้องพึ่งพาซอฟต์แวร์ราคาแพงจากต่างประเทศ ทำให้การสื่อสารด้วย VoIP ไม่จำกัดอยู่แค่ในองค์กรที่มีขนาดใหญ่และมีงบประมาณในการลงทุนสูงอีกต่อไป

เนื่องจากซอฟต์แวร์ FreeSWITCH มีการพัฒนาเปลี่ยนผ่านรุ่น อย่างรวดเร็วซึ่งในขณะที่งานวิจัยนี้ได้ศึกษาทดลองอยู่นั้นได้เลือกใช้รุ่น 1.2.6 เนื่องจากเป็นรุ่นที่มีความเสถียรและคงที่ในขณะนั้น ดังนั้นจึงเลือกใช้รุ่น 1.2.6 ในการเป็นฐานพัฒนาต่อยอด แต่ในขณะกำลังเขียนบทความนี้ (กุมภาพันธ์ พ.ศ. 2558) มีรุ่น 1.4.14 ออกมาล่าสุด งานวิจัยจึงได้ทดสอบประสิทธิภาพทางด้านความมั่นคงตามแบบการทดสอบในงานวิจัย[22] ซึ่งผลการทดลองเห็นได้ว่า FreeSWITCH รุ่น 1.4.14 ยังคงมีปัญหาด้านความมั่นคงไม่ต่างจากรุ่น 1.2.6 ที่ใช้ในงานวิจัยนี้

แนวทางการวิจัยและพัฒนาต่อยอด ISANBox.F V.2 คือ สืบเนื่องจากการเข้ารหัสข้อมูลเสียงเพื่อแก้ไขปัญหาการดักฟังนั้น งานวิจัยได้พบว่าในทางเทคนิคการแลกเปลี่ยนกุญแจของโพโทคอล SRTP ยังมีปัญหาที่ทำให้กุญแจลับที่ใช้ในการเข้าและถอดรหัสข้อมูลเสียง อาจจะรั่วไหลไปยังผู้ไม่หวังดีและอาจเกิดปัญหาด้านความมั่นคงตามมา ซึ่งงานวิจัยในอนาคตจะได้ศึกษาและพัฒนาพร้อมเสนอแนวทางแก้ไขปัญหาดังกล่าวต่อไป

กิตติกรรมประกาศ

งานวิจัยนี้ต้องขอขอบคุณ หลักสูตรวิทยาศาสตรมหาบัณฑิต วิทยาการคอมพิวเตอร์ คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม ที่สนับสนุนทางด้านอุปกรณ์และสถานที่ในการทำวิจัยในครั้งนี้จนสำเร็จไปได้ด้วยดี

เอกสารอ้างอิง

1. คณะกรรมการกิจการโทรคมนาคมแห่งชาติ. การให้บริการเสียงผ่านการให้บริการอินเทอร์เน็ต. [online]. 2012 [cited 13 December 2014]; http://www.nbtc.go.th/wps/portal/NTC/Law/LawRelating/Announcement.
2. Asterisk. [online]. 2013 [cited 9 December 2014]; http://www.asterisk.org.
3. FreeSWITCH. [online]. 2012 [cited 9 December 2014]; http://www.freeswitch.org
4. Kamailo. [online]. December 2014 [cited 9 December 2014]; http://www.kamailio.org.
5. SIP TLS for FreeSWITCH. [online]. 2013 [cited 20 December 2014]; http://wiki.freeswitch.org/wiki/SIP_TLS.
6. Norrman K, Baugher M. The Secure Real-time Transport Protocol (SRTP). IETF, RFC 3711, Mach 2004.
7. Xianglin D, Chien-wei L. Security of VoIP SIP flooding and its Mitigation. Proceeding of New Zealand Computer Science Research Student Conference April 2008; Christchurch New Zealand; pp. 207-207.
8. ปิยวัจน์ ค้าสบาย, สมนึก พ่วงพรพิทักษ์. การประเมินปัญหาด้านความมั่นคงของซอฟท์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพี. การประชุมวิชาการทางคอมพิวเตอร์และเทคโนโลยีสารสนเทศ(CIT); จันทบุรี:มหาวิทยาลัยบูรพา; มกราคม 2553; หน้า 33-38.
9. ประดิษฐ์ วงศ์สกุล, ปิยะณัฐ สุยังกุล, สมนึก พ่วงพรพิทักษ์. ระบบให้บริการโทรศัพท์ผ่านอินเทอร์เน็ตแบบมั่นคงโดยการต่อยอดฟรีสวิตช์. การประชุมวิชาการทางคอมพิวเตอร์และเทคโนโลยีสารสนเทศ (CIT); เชียงใหม่; กุมภาพันธ์ 2556; หน้า 63-69.
10. Asterisk vs. FreeSWITCH. [online]. 2013 [cited 23 December 2014]; http://anders.com/cms/266.
11. มี Open-source VoIP อะไรให้เลือกใช้ได้บ้าง. [online]. June 2012 [cited 17 December 2014]; http://www.asteriskdiy.com.

12. Sofia-SIP Library. [online]. March 2014 [cited 9 January 2014]; http://sofia-sip.sourceforge.net/.
13. Schulzrinne H, Casner S. RTP: A Transport Protocol for Real-Time Applications. IETF, RFC 3550, July 2003.
14. Dierks T. The Transport Layer Security (TLS) IETF, RFC 2246, March 2008.
15. Redhat.com. Certificates and Authentication. [online]. 2013 [cited 21 December 2014]; https://access.redhat.com.
16. Petraschek M. Security and Usability Aspects of Man-in-the-Middle Attack on ZRTP. Journal of Universal Computer Science (JUCS) 2008; pp. 673-692.
17. Puangpronpitag S, Kasabai P. MSDES: More SDES Key Agreement for SRTP. International Journal of Computer Theory and Engineering; October 2012; Chengdu China; pp. 777-780.
18. คธาวุฒิ จันบัวลา, สมนึก พ่วงพรพิทักษ์. Extended Development of Open-Source Software Package. การประชุมวิชาการ งานวิจัยและพัฒนาเชิงประยุกต์ ECTI-CARD 2012; ปทุมธานี; หน้า 58-63.
19. BlueBox Project. [online]. 2013 [cited 17 December 2014]; http://2600hz.org/.
20. ประดิษฐ์ วงศ์สกุล, สมนึก พ่วงพรพิทักษ์. การประเมินคุณภาพการให้บริการวีโอไอพีโอเพนซอร์ซอฟต์แวร์ Asterisk VS. FreeSWITCH VS. Kamailo. การประชุมวิชาการระดับประเทศด้านเทคโนโลยีสารสนเทศ NCIT2013; 2556; เพชรบุรี; หน้า 119-124.
21. 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.
22. 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.
23. สาโรจน์ ยิ่งศักดิ์มงคล, ธนัญ จารุวิทยโกวิทม. ความจุระบบการใช้งานโทรศัพท์ผ่านอินเทอร์เน็ตบนโครงข่ายไร้สายแบบเมชประเภทกริด. การประชุมวิชาการเสนอผลงานวิจัยระดับบัณฑิตศึกษาแห่งชาติ; ธันวาคม 2554; ขอนแก่น: มหาวิทยาลัยราชมงคลอีสาน; หน้า 128-134.
24. ITU-T Recommendation P.800. Methods for subjective determination of transmission quality. [online]. 2006 [cited 4 july 2014]; www.itu.int/rec/T-REC-P.800-199608-l/en.
25. ITU-T Recommendation G.107. The E-Model a computational model for use in transmission planning. [online]. 2003 [cited 4 july 2014]; http://www.itu.int/rec/T-REC-G.107.
26. คณะกรรมการกิจการโทรคมนาคมแห่งชาติ. มาตรฐานสำหรับการให้บริการเสียงผ่านการให้บริการอินเทอร์เน็ต. [online] .2013 [cited 18 December 2014]; http://standard.nbtc.go.th/.
27. Commview. [online]. 2014 [cited 22 December 2014]; http://www.tamos.com/products/commview/.