การจำกัดและป้องกันสายไม่พึงประสงค์ของการใช้บริการโทรศัพท์ผ่านอินเตอร์เน็ตโดยการระบุและปิดกั้น URI ของโพรโตคอล SIP

โดย

ศิวะพร วิวัฒน์ภิญโญ

พรประสิทธิ์ บุญทอง

ศิริเรือง พัฒน์ช่วย

อาทิตย์ อยู่เย็น

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

Copyright © by Rajamangala University of Technology Rattanakosin

All rights reserved

สนับสนุนงบประมาณโดย

มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

ประจำปีงบประมาณ 2557

THE DEVELOPER SELF-DIRECTED LEARNING SYSTEM OF STUDENT USING MULTIMEDIA ON WEB

By

Siwaphon Viwatpinyo

Pornprasit Boontong

Siriruang Phatchuay

Arthit Yooyen

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

Copyright © by Rajamangala University of Technology Rattanakosin

All rights reserved

Granted by

Rajamangala University of Technology Rattanakosin

Fiscal year 2014

กิตติกรรมประกาศ

งานวิจัยนี้จะสำเร็จได้ด้วยดีมิได้ หากขาดการสนับสนุนงบประมาณและเวลา จากมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ โดยผู้วิจัยได้รับการสนับสนุนงบประมาณแผนดินประจำปี 2557 ดังนั้นคณะผู้วิจัยจึงขอขอบคุณสำหรับการสนับสนุนในครั้งนี้ด้วย

ศิวะพร วิวัฒน์ภิญโญ และ คณะ

สิงหาคม 2557

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

Copyright © by Rajamangala University of Technology Rattanakosin

All rights reserved

บทคัดย่อ

รหัสโครงการ : A35/ 2557

ชื่อโครงการ : การจำกัดและป้องกันสายไม่พึงประสงค์ของการใช้บริการโทรศัพท์ผ่านอินเตอร์เน็ตโดยการการระบุและปิดกั้น URI ของโพรโตคอล SIP

ชื่อนักวิจัย : นายศิวะพร วิวัฒน์ภิญโญ นายพรประสิทธิ์ บุญทอง นางสาวศิริเรือง พัฒน์ช่วย **และ**นายอาทิตย์ อยู่เย็น

งานวิจัยนี้มีวัตถุประสงค์เพื่อสร้างกลไกเพื่อทำหน้าที่ป้องกันการโทรจากผู้ไม่หวังดี(SPIT)ไปสู่ผู้ใช้งานโทรศัพท์ผ่านอินเตอร์เน็ตทั่วไป โดยการพัฒนาส่วนของโปรแกรมที่ทำงานร่วมกับการทำงานปกติของชุดโปรแกรม Asterisk ซึ่งทำหน้าที่เป็น VoIP Gateway โดยโปรแกรมที่พัฒนาขึ้นมาจะมีกลไลการตรวจสอบสองส่วนคือ 1)ตรวจสอบจากพฤติกรรมปกติของการโทรคือหากเลขหมายปลายทางนั้นเป็นเลขหมายที่เคยมีการติดต่อเข้ามายังเลขหมายต้นทางก่อนหน้านี้ก็เชื่อได้ว่าการโทรดังกล่าวนั้นเป็นการโทรปกติที่มีการโทรโต้ตอบกันอยู่แล้วระบบก็จะทำการบันทึกเลขหมายดังกล่าวไว้ในรายการสีขาว (White list) ซึ่งเลขหมายดังกล่าวเป็นการโทรปกติระบบก็จะอนุญาตให้ติดต่อไปยังเลขหมายปลายทางได้ 2)ตรวจสอบจากความผิดปกติของการโทรจากต้นทางไปยังปลายทางโดยอาศัยการตรวจสอบจำนวนครั้งของการโทรที่มีความพยายามโทรไปยังเลขหมายปลายทางหลายๆหมายเลขจากเลขหมายต้นทางเดียวในช่วงเวลาที่สม่ำเสมอตลอดเวลา ก็จะสามารถระบุเบื้องต้นได้ว่าการโทรดังกล่าวคือการโทรที่ไม่พึงประสงค์ ระบบก็จะทำการบันทึกเลขหมายดังกล่าวไว้ในรายการสีดำ (Black list) ซึ่งเลขหมายดังกล่าวจะถูกตัดการติดต่อทันทีเพื่อไม่ให้ไปรบกวนผู้ใช้บริการเป้าหมายได้อีกซึ่งเมื่อเลขหมายเดิมติดต่อผ่านเข้ามาอีกก็จะสามารถสรุปได้ในทันทีว่าเป็นการโทรปกติหรือไม่ปกติโดยใช้ White list และ Black list

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

Copyright © by Rajamangala University of Technology Rattanakosin

All rights reserved

คำสำคัญ : โทรศัพท์ผ่านอินเตอร์เน็ต, ซิปโปรโตคอล, สปริท

E-mail Address : siwaphon.viw@rmutr.ac.th

ระยะเวลาโครงการ : ตุลาคม 2556 – กันยายน 2557

Abstract

Code of project : **A35/ 2557**

Project name : LIMIT AND PREVENT THE UNWANTED USE OF THE INTERNET PHONE SERVICE BY IDENTIFYING AND BLOCKING THE URI OF THE SIP PROTOCOL

Researcher name : Mr.Siwaphon Viwatpinyo, Mr.Pornprasit Boontong
Miss.Siriruang Phatchuay, Mr.Arthit Yooyen

This research aims to establish a mechanism to prevent disgruntled calls(SPIT) over the Internet to general users. By the development of the program Work with the normal operation of the program Asterisk VoIP Gateway, who serves as the program developed monitoring mechanism will be two parts. 1) Check the normal behavior of the call If the destination number is a number used to connect to the incoming previously believe that such a call is a normal call interact with each other already, it will record them in the white list. The numbers above the normal call system will allow the interface to the destination number. 2)detection of abnormalities of the call from the source to the destination by checking the number of the caller is trying to call multiple numbers of same incoming numbers at time can indicate that the caller is unsolicited call. System, it will record them in the black list. This caller will be disconnected immediately so as not to interfere with target callee which when same caller connect again, it can be concluded immediately that it was normal or abnormal by use the White list and Black list.

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

Keywords: VoIP, SIP Protocol, SPIT.

E-mail Address : **siwaphon.viw@rmutr.ac.th**

Period of project : October 2013 – September 2014

สารบัญ

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

สารบัญ(ต่อ)

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

Copyright © by Rajamangala University of Technology Rattanakosin

All rights reserved

สารบัญตาราง

หน้า

ตารางที่

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

สารบัญภาพ

หน้า

ภาพที่

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

บทที่ 1
บทนำ

การใช้งานโทรศัพท์ผ่านเครือข่ายอินเตอร์เน็ตในปัจจุบันนั้นได้รับความนิยมอย่างมากจนเริ่มมีผู้ให้บริการโทรศัพท์พื้นฐานใหญ่ๆ เช่น ทรู ทีโอที และ แคทเทเลคอม หันมาให้บริการมากขึ้นทุกวัน เนื่องจากค่าใช้จ่ายต่อการโทรในแต่ละครั้ง นั้นถูกกว่าระบบโทรศัพท์ธรรมดารวมทั้งยังสามารถเพิ่มการใช้งานในส่วนของการโทรศัพท์แบบภาพวีดีโอได้อีกด้วย แต่ปัญหาที่ตามมาในปัจจุบันนั้นก็คือปัญหาด้านความเป็นส่วนตัวของผู้ใช้งานทั่วไปและการสร้างความรำคาญในการใช้บริการ เช่น เมื่อมีผู้คิดที่จะทำการโฆษณาสินค้าหรือบริการผ่านทางระบบโทรศัพท์ผ่านอินเตอร์เน็ตโดยการโทรจากระบบอัตโนมัติไปยังผู้ใช้งานทั่วไปเมื่อผู้ใช้ทั่วไปรับสายก็จะมีการเล่นไฟล์เสียงโฆษณานั้นๆ ร่วมทั้งยังสามารถสร้างระบบอัตโนมัติที่เป็นแบบโต้ตอบกับผู้ใช้ได้เพื่อทำการรับสั่งซื้อสินค้าหรือบริการ แต่ในบางครั้งการโทรแบบนี้ก็เกิดขึ้นบ่อยมากเกินไปกับผู้ใช้คนเดิมซึ่งทำให้เกิดความรำคาญและไม่เป็นส่วนตัวแก่ผู้ใช้บริการ ซึ่งจะส่งผลให้เกิดความไม่น่าเชื่อถือต่อระบบของผู้ให้บริการซึ่งอาจนำมาซึ่งการเปลี่ยนผู้ให้บริการ ก็จะเป็นสาเหตุให้ผู้ให้บริการที่ไม่ดูแลในเรื่องนี้ให้ดีเสียลูกค้าได้

1. ความเป็นมาและความสำคัญของปัญหา

ปัญหาของผู้ใช้งานระบบโทรศัพท์ผ่านอินเตอร์เน็ตในปัจจุบันคือความรำคาญและการละเมิดความเป็นส่วนตัวของผู้ใช่งานจากผู้ที่มีวัตถุประสงค์ด้านการโฆษณาและการขายสินค้าหรือบริการผ่านทางดังที่ได้กล่าวมาแล้วนั้น ถือเป็นการโจมตีไปยังยังผู้ใช้งานที่เรียกว่าสปริท(SPIT : Spam over Internet Telephony) สปริทนั้นก็คล้ายกับสแปมอีเมล์(Spam Mail) ซึ่งจะก่อความรำคาญแก่ผู้ใช้งานเนื่องจากไม่ได้เกิดจากความต้องการของผู้ใช้งานนอกจากนี้มันยังก่อให้เกิดการใช้งานที่ไม่ปกตินั้นก็คือเมื่อการโทรเกิดจากระบบอัตโนมัติดังนั้นการโทรจะเกิดขึ้นอยู่ตลอดเวลาซึ่งทำให้เกิดปัญหาการด้านภาระการให้บริการกับเครื่องแม่ข่ายของระบบผู้ให้บริการได้

ปัญหาความเชื่อมั่นต่อผู้ให้บริการก็ถือเป็นปัญหาใหญ่ที่อาจทำให้รายได้ของผู้ให้บริการลดลงซึ่งอาจเกิดจากความไม่เชื่อใจและเลิกใช้บริการของลูกค้าเอง แต่ผู้ให้บริการกลับต้องแบกรับภาระค่าใช้จ่ายในการซ่อมบำรุงระบบเพื่อให้บริการอยู่เหมือนเดิม สาเหตุที่ผู้โจมตีซึ่งก็คือผู้ที่ต้องการโฆษณาสินค้าเพื่อขายสินค้าหรือบริการต่างๆนั้น หันมาใช้งานการโทรศัพท์ผ่านอินเตอร์เน็ตเนื่องจากปัจจุบันค่าใช้จ่ายในการโทรของโทรศัพท์ปกตินั้นแพงกว่าโทรศัพท์ผ่านอินเตอร์เน็ตมากอีกทั้งการ

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

สร้างระบบอัตโนมัติเพื่อโทรไปหาลูกค้าก็สามารถสร้างได้ง่ายกว่าต้นทุนถูกกว่าและการเพิ่มจำนวนคู่สายการโทรก็ทำได้ง่ายกว่าในราคาที่ถูกกว่าเช่นกัน

จากปัญหาที่กล่าวมาข้างต้น จะเห็นว่าหากมีการตรวจสอบการโทรจากผู้ให้บริการ ซึ่งก็คือต้นทางของการติดต่อ เมื่อมีการตรวจสอบพบว่าผู้ใช้รายใดมีลักษณะการใช้งาน หรือพฤติกรรมการโทรที่ตรงกับการทำงานของ SPIT ก็ให้ทำการปิดกันการติดต่อไปยังผู้ใช้รายอื่นๆ ในการตรวจสอบนั้นจะอาศัยการวิเคราะห์ค่าสถิติของการโทรซึ่งผู้ใช้โดยทั่วไปจะมีพฤติกรรมการโทรที่ไม่บ่อยและไม่ถี่มาก แต่หากเป็น SPIT จะมีการโทรไปยังปลายทางอย่างต่อเนื่อง เรียงไปตามหมายเลขที่มีการตั้งค่าไว้และใช้เวลาทั้งวันในการโทร จากลักษณะพฤติกรรมตรงนี้ผู้วิจัยจึงพัฒนาโปรแกรมขึ้นมาเพื่อให้ทำหน้าที่ตรวจสอบโดยการเปรียบเทียบเวลาในการโทรที่บ่อยเกินไป ซึ่งระบบจะสามารถตรวจพบและปิดกันไม่ให้ SPIT โทรไปยังปลายทางได้ นอกจากนี้ยังสร้างส่วนของการตรวจสอบการโทรที่เป็นปกติขึ้นมาอีกด้วยโดยพิจารณาจากพฤติกรรมการโทรที่หมายเลขปลายทางนั้น เป็นหมายเลขที่เคยโทรเข้ามาก่อนหน้านี้ซึ่งก็จะสรุปได้ว่าการโทรออกในครั้งนี้เป็นการโทรแบบปกติ

2. วัตถุประสงค์การวิจัย

เพื่อศึกษาและพัฒนาระบบที่จะทำหน้าที่ตรวจสอบและป้องกันการโทรที่เป็น SPIT ซึ่งก็คือสายโทรที่ไม่พึงประสงค์โดยอาศัยกลไกการตรวจสอบค่าสถิติการโทรของ SIP URI เพื่อปิดกันการใช้บริการจาก URI ที่ตรวจพบว่าน่าจะเป็น SPIT

3. กรอบแนวคิดการวิจัย

การโทรศัพท์ผ่านอินเตอร์เน็ต (VoIP) นั้นทุกการโทรจำเป็นต้องระบุ SIP URI ต้นทางและปลายทางเช่นเดียวกับหมายเลขโทรศัพท์ปกติ ดังนั้นจะสามารถตรวจสอบลักษณะการโทรทุกๆ คู่สายได้ เพื่อระบุว่าการโทรใดเป็นการโทรแบบปกติและการโทรใดเป็นการโทรที่ไม่ปกติที่เรียกว่า SPIT

โดยกระบวนการตรวจสอบจะมีลำดับขั้นตอนดังนี้

1. เมื่อมีการโทรเกิดขึ้น VoIP Gateway จะทำการตรวจสอบ SIP URI ที่เป็นต้นทาง (A) และปลายทาง (B) ว่าก่อนหน้านี้เคยมีการติดต่อกันมาก่อนหรือไม่เช่น B เคยโทรมาหา A หรือไม่ หากว่ามีการติดต่อกันมาก่อนก็จะถือว่าเป็นการโทรปกติและจะบันทึก SIP URI ของ A ไว้ในฐานข้อมูล Whitelist

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

2. หากการโทรจาก A ไปยัง B ไม่เคยมีการติดต่อกันมาก่อนขั้นแรกจะนำ SIP URI ของ A ไปตรวจสอบกับฐานข้อมูล Blacklist หากพบ SIP URI ของ A ก็จะยุติการโทรดังกล่าวก่อนที่จะมีการติดต่อไปยังปลายทางทันที

3. หากไม่พบ SIP URI ของ A ทั้งในรายการ Whitelist และ Blacklist ก็จะบันทึก SIP URI ของ A ไว้ใน Graylist ซึ่งหาก SIP URI ของ A ได้เคยถูกบันทึกในรายการ Graylist ในครั้งต่อไปก็จะเพิ่มค่าของ Count ในข้อมูลของ SIP URI ของ A เพื่อนำไปตรวจสอบกับช่วงเวลาที่กำหนดหากมีอัตราความถี่ในการโทรบ่อยเกิดกว่าเกณฑ์ SIP URI ของ A จะถูกสรุปให้เป็น SPIT และจะถูกย้ายไปบันทึกในรายการ Blacklist แทน

จากขั้นตอนวิธีการดังที่กล่าวมาจะสามารถตรวจสอบได้ว่าการโทรใดเป็น SPIT และการโทรใดเป็นการโทรแบบปกติซึ่งจะลดโอกาสที่การโทรเพื่อก่อความรำคาญต่อผู้ใช้งานทั่วไปจะหลุดรอดไปยังผู้ใช้ได้

4. ผลการวิจัยที่คาดว่าจะได้รับ

จากการวิจัยโมดูลที่พัฒนาขึ้นมาให้ทำงานร่วมกับ VoIP Gateway ที่เป็นชุดโปรแกรม Asterisk จะทำการตรวจสอบการโทรจากต้นทางไปยังปลายทางโดยระบุได้ว่าการโทรใดเป็นการโทรปกติโดยตรวจสอบจากพฤติกรรมของผู้ใช้ที่เคยโทรไปหาเลขหมายใดๆ และการโทรใดเป็น SPIT จากการเก็บข้อมูลจำนวนครั้งการโทรต่อช่วงเวลาทั้งนี้หากการโทรดังกล่าวมีจำนวนครั้งการโทรไปยังหมายเลขใดๆ มากกว่าเกณฑ์ที่กำหนดในช่วงเวลาที่กำหนดก็จะสรุปว่าสายโทรดังกล่าวเป็น SPIT และจะบันทึก SIP URI นั้นไว้เพื่อที่หากมีการโทรจาก SIP URI เดิมอีกก็จะถูกปิดกันในทันทีโดย VoIP Gateway

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

1. VoIP (Voice over IP)

คือการโทรศัพท์ผ่านอินเทอร์เน็ต (Internet Telephone) เป็นเทคโนโลยีที่ช่วยให้การสื่อสารด้วยเสียง สามารถทำได้โดยผ่านเครือข่ายอินเทอร์เน็ต ซึ่งเทคโนโลยีนี้ จะทำให้ช่วยประหยัดค่าใช้จ่ายในการใช้โทรศัพท์ติดต่อสื่อสาร โดยสามารถที่จะโทรหากันได้ไม่จำกัดเวลา โดยไม่มีค่าใช้จ่ายในการโทรศัพท์ ผ่านการเชื่อมต่ออินเทอร์เน็ต ไปได้ทุกจุดหมายทั่วโลก เพียงแต่ปลายทางต้องมีการเชื่อมต่อเข้าอินเทอร์เน็ต และใช้บริการ VoIP ในเครือข่ายเดียวกัน โดยอาศัยซอร์ฟแวร์โทรศัพท์เช่น X-lite หรือใช้งานผ่านเครื่องโทรศัพท์เฉพาะที่สามารถเชื่อมต่อสัญญาณอินเตอร์เน็ตเพื่อเข้าสู่ระบบ VoIP ได้โดยมีส่วนประกอบคือ

1.1 VoIP Client เป็นอุปกรณ์ที่เป็นแบบใช้ได้โดยตรง ผ่านเครือข่ายอินเตอร์เน็ต โดยไม่ต้องพึ่งพาคอมพิวเตอร์ (Stand Alone) อุปกรณ์ที่จำเป็นต้องใช้ในการสื่อสารสำหรับด้านลูกข่าย (Client) แบ่งได้ดังต่อไปนี้

1.1.1 เครื่องโทรศัพท์ไอพี (IP Phone) เป็น อุปกรณ์ที่ต่อกับเครือข่าย แล้วใช้ได้ทันที ซึ่งอุปกรณ์ชนิดนี้ รูปร่างลักษณะจะเหมือนโทรศัพท์ทั่วๆไป แต่แทนที่จะเสียบสายโทรศัพท์เข้าตัวเครื่องจะใช้เป็นสาย LAN เชื่อมต่อแทน

1.1.2 กล่องแปลงสัญญาณเสียง (VoIP Gateway / ATA Adapter) จะเป็นกล่องสำหรับเชื่อมต่อเข้าระบบเครือข่าย โดยจะใช้สาย LAN เชื่อมต่อเข้ากับกล่องในส่วนขาเข้า และจะมีที่สำหรับเสียบสายโทรศัพท์ออกจากกล่อง โดยกล่องชนิดนี้ ใช้สำหรับเชื่อมต่อเข้ากับโทรศัพท์ธรรมดาทั่วๆไป และใช้งานได้ทันที หรือ จะต่อเข้ากับตู้สาขา เปรียบเสมือนเป็นสายนอก (CO Line) สายหนึ่ง เพื่อโทรออกไปปลายทาง จากเครื่องต่อพ่วงหลายๆเครื่องก็ได้

1.2 VoIP to PSTN Gateway สำหรับการใช้งาน VoIP โดยเชื่อมต่อกับโทรศัพท์พื้นฐาน หรือโทรศัพท์มือถือ ทั้งในและต่างประเทศ สามารถประหยัดค่าใช้จ่ายได้มาก โดยสมัครใช้งานผ่าน VoIP Gateway ต่างประเทศ โดยซื้อเป็นบัตรเติมเงินล่วงหน้า และสามารถโทรเข้าโทรศัพท์พื้นฐานทั่วโลก ในราคาประหยัด ขอแนะนำบริการ CALLCENTRIC ซึ่งมีค่าใช้จ่ายในการโทรต่อนาทีที่ต่ำ (ดูอัตราค่าโทรได้ที่นี่) และไม่มีค่าใช้จ่ายรายเดือน สำหรับบริการ Pay Per Call รวมไปถึงมีบริการโทรได้ไม่จำกัด สำหรับโทรศัพท์ในประเทศสหรัฐอเมริกา สำหรับบริการ North America Unlimited

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

($19.95/เดือน) และ โทรได้ไม่จำกัด ใน 39 ประเทศทั่วโลก สำหรับบริการ World Select ($29.95/เดือน)

1.3 VoIP Server มาตรฐานสำหรับ VoIP นั้น จะมีมาตรฐาน หรือ Protocol หลักที่นิยมใช้กันอยู่ 2 ประเภท ก็คือ H.323 และ SIP โดยมาตรฐาน SIP นั้นปัจจุบัน มีการนิยมใช้สูงมาก ซึ่งอุปกรณ์สำหรับ VoIP ที่ออกใหม่ๆ จะมีการรองรับมาตรฐาน SIP สำหรับการตั้ง SIP Server ส่วนตัวนั้น สามารถที่จะซื้อเป็น VoIP Server สำเร็จรูปไปใช้ หรือ อาจจะหาเครื่องสำหรับทำ Server แล้วติดตั้งโปรแกรมเพื่อแปลง Server ดังกล่าวให้เป็น SIP Server ก็สามารถทำได้ เพียงแต่ข้อควรคำนึงถึงคือถ้าต้องการใช้งาน SIP Server เพื่อใช้งานกับ VoIP Client ในต่างเครือข่าย โดยต้องผ่านอินเทอร์เน็ต ตัว SIP Server นั้น ต้องมี Public IP ที่เป็นแบบ Static IP เพื่อที่ว่าเครื่องลูกข่ายจะสามารถที่จะเชื่อมต่อเข้ามาลงทะเบียนได้ แต่ถ้าเป็นเครือข่ายภายในองค์กรเอง และใช้สำหรับสื่อสารเฉพาะภายในองค์กร ก็สามารถกระทำได้โดยไม่มีปัญหาโดยใช้ Private IP นอกจากนี้ VoIP Server ยังสามารถทำงานในลักษณะต่อไปนี้ได้

1.3.1 ระบบตู้สาขาผ่านเครือข่าย (IP-PBX System / Communication Server)

1.3.2 ระบบเชื่อมต่อตู้สาขาผ่านเครือข่าย (Inter-Branch Voice Trunking System / PBX Link System)

1.3.3 ระบบโต้ตอบด้วยเสียงอัตโนมัติ (Interactive Voice Response / IVR Server)

2. รูปแบบการใช้งาน VoIP (Voice over Internet Protocol)

สำหรับรูปแบบบริการของ Voice over IP สามารถทำได้หลายวิธีซึ่งแล้วแต่การเลือกใช้งานหรือความสะดวกในการใช้งาน

2.1 จากเครื่องคอมพิวเตอร์ไปสู่เครื่องคอมพิวเตอร์ (PC-to-PC) โดยวิธีการนี้จำเป็นต้องอาศัยเครื่องคอมพิวเตอร์ทั้งต้นทางและปลายทาง พร้อมทั้งติดตั้งโปรแกรมเดียวกัน หรือติดตั้งโปรแกรมที่สามารถใช้งานร่วมกันได้ ซึ่งรูปแบบนี้เป็นวิธีการสื่อสารที่ไม่ต้องเสียค่าบริการโทรศัพท์แต่อย่างใดเลย แต่ต้องนัดแนะเวลาในการใช้อินเทอร์เน็ตในเวลาเดียวกันเนื่องจากไม่สามารถส่งสัญญาณเรียกไปยังคอมพิวเตอร์ที่ปิดอยู่ได้

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

ภาพที่ 1 การใช้งาน VoIP แบบ PC-to-PC[9]

2.2 จากเครื่องคอมพิวเตอร์สู่เครื่องโทรศัพท์ (PC-to-Phone) เป็นรูปแบบที่ใช้ได้กับผู้ใช้ต้นทางที่มีเครื่องคอมพิวเตอร์และโปรแกรมโทรศัพท์ โดยผู้รับปลายทางนั้นใช้เครื่องโทรศัพท์ธรรมดา แต่วิธีนี้ต้องอาศัยผู้ให้บริการในการเชื่อมต่อระบบอินเตอร์เน็ตเข้ากับระบบเครือข่ายโทรศัพท์ท้องถิ่น (Internet Telephone Service Provider หรือ ITSP) โดยผู้ใช้บริการต้องเสียค่าบริการตามเวลาที่ใช้งานจริง

ภาพที่ 2 การใช้งาน VoIP แบบ PC-to-Phone[9]

2.3 จากเครื่องโทรศัพท์สู่เครื่องคอมพิวเตอร์ (Phone-to-PC) วิธีการนี้ใช้หลักการเช่นเดียวกันกับ PC-to-Phone แต่ต้นทางจะเป็นเครื่องโทรศัพท์ธรรมดา ขณะที่ปลายทางนั้นเป็นเครื่องคอมพิวเตอร์และโปรแกรมโทรศัพท์แทน ซึ่งผู้ใช้งานต้องเสียค่าบริการตามที่ใช้งานจริงเช่นเดียวกัน และต้องนัดแนะเวลาในการใช้เนื่องจากไม่สามารถส่งสัญญาณเรียกไปยังคอมพิวเตอร์ที่ปิดอยู่ได้

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

ภาพที่ 3 การใช้งาน VoIP แบบ Phone -to-PC[9]

2.4 จากเครื่องโทรศัพท์สู่เครื่องโทรศัพท์ (Phone-to-Phone) เป็นวิธีที่ผู้ใช้โทรศัพท์สามารถเรียกไปยังโทรศัพท์อีกเครื่องหนึ่งได้เหมือนในกรณีทั่วๆ ไป แต่สัญญาณจะถูกแปลงให้อยู่ในรูปข้อมูล IP แล้วส่งผ่านเครือข่ายสัญญาณข้อมูลบนอินเทอร์เน็ต โดยกรณีนี้จะได้คุณภาพเสียงคมชัดและผู้ใช้

สามารถใช้โทรศัพท์ได้ตามปกติไม่ต้องนัดแนะเวลาในการใช้เนื่องจากไม่ต้องส่งสัญญาณเรียกไปยังคอมพิวเตอร์ทำให้สะดวกต่อการใช้งาน

ภาพที่ 4 การใช้งาน VoIP แบบ Phone -to- Phone[9]

3. VoIP Spam/SPIT (Spam Over Internet Telephony)

VoIP Spam หรือ SPIT นั้นหมายถึงข้อความที่ไม่พึงประสงค์ของผู้ใช้งาน VoIP เนื่องจากมันก่อความรำคาญและก่อปัญหาแก่การจราจรทางอินเตอร์เน็ตเนื่องจากส่วนใหญ่แล้ว VoIP Spam คือการโทรจากระบบอัตโนมัติซึ่งได้ทำการบันทึกเสียงสนทนา ที่เป็ฯข้อมูลที่ต้องการให้ผู้รับสายได้ฟังเพื่อจุดประสงค์ต่างๆ เช่นการโฆษณาให้ซื้อสินค้า หรือบริการต่างๆ รวมถึงการชวนเชื่อเพื่อให้สมัครสมาชิกเพราะจะได้รับการบริการ ซึ่ง VoIP Spam นั้นไม่สนว่าผู้รับสายยินดีและยินยอมรับฟังข้อมูลต่างๆ เหล่านี้หรือไม่ และหากมีการโทรเข้ามาจาก VoIP Spam เป็นจำนวนมากในแต่ละวันก็อาจทำให้ผู้รับสายต้องเกิดความติดขัดหรือพลาด ในการสื่อสารกับบุคคลที่จำเป็นจริงๆ เนื่องจาก VoIP Spam จะทำให้คู่สายนั้นไม่ว่าง

4. Asterisk

คือ open source software ที่ทำหน้าที่หลักเป็น Soft switch, IP-PBX หรือที่เรียกว่าตู้ชุมสายโทรศัพท์ระบบ IP ซึ่งมีหน้าที่ในการควบคุมและจัดการบริหาร การเชื่อมต่อ ระหว่างอุปกรณ์โทรศัพท์ผ่านเครื่องข่ายเนทเวอร์ค อีกทั้งยังสามรถเพิ่มเติมประสิทธิ์ภาพและความสามารถในการทำงานได้โดยง่าย ตัวอย่างการนำ Asterisk ไปใช้งานเช่น

4.1. Asterisk as a switch (PBX) ทำหน้าที่เป็น IP PBX ทำหน้าที่เชื่อมต่อระหว่าง Client เข้าด้วยกันในเครือข่ายอินเตอร์เน็ต สามารถทำงานในระบบปฏิบัติการได้หลากหลายเช่น Linux, Mac OS X, OpenBSD, FreeBSD, Sun Solaris มี Feature มากมายตามที่ได้กล่าวมาแล้ว โครงสร้างของ Asterisk มีความยืดหยุ่นนั้นคือรองรับหลายโปรโตคอล และยังเชื่อมต่อกับอุปกรณ์ที่รองรับ IP telephony ได้เกือบทุกชนิด

4.2. Asterisk as a gateway สามารถนำ Asterisk เชื่อมต่อระบบโทรศัพท์เครือข่ายอินเตอร์เน็ตกับระบบโทรศัพท์แบบ PSTN ได้ รองรับหลาย Protocol และMedia Codec

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

4.3. Asterisk as a feature/media server สามารถนำ Asterisk ทำหน้าที่เป็นระบบตอบรับอัตโนมัติ IVR Interactive Voice Response สามารถจัดห้องประชุมผ่านทางเครื่อยข่ายโทรศัพท์ แทนที่ระบบ Voice Mail ที่ล้าสมัย ระบบการส่งข้อความ หรือ ประยุกต์ให้หน้าเวปรองรับ Telephony

4.4. Inter Asterisk exchange protocol IAX2 เป็น โปรโตคอลที่ออกแบบมาเพื่อสร้าง ปรับเปลี่ยน สิ้นสุด Multimedia Sessions ในเครือข่ายอินเตอร์เน็ต ถูกพัฒนาโดย Open source Community เพื่อใช้กับ Asterisk PBX โดยเน้นในการส่ง VoIP แต่ IAX2 สามารถใช้ Stream video ได้อีกด้วย IAX2 รวมการส่ง Control และ Media ในโปรโตคอลเดียวใช้โปรโตคอล UDP port 4569 ซึ่งเป็นข้อสำคัญที่ทำให้ IAX2 สามารถส่งสัญญาณผ่าน NAT Network Address Translation โดยที่ไม่ต้องการปรับเปลี่ยนเพิ่มเติม IAX2 รวมสัญญาณและ Data เข้าด้วยกันทำให้ลด Bandwidth เมื่อเทียบกับการใช้โปรโตคอล SIP และ RTP ซึ่งเป็นประโยชน์สำคัญในการนำไปใช้ ใน IP telephony เพราะต้องรองรับการใช้งานได้ในจำนวนมาก และประโยชน์สำคัญอีกข้อหนึ่งคือในสำนักงานบริษัทจะใช้ NAT ซึ่ง IAX2 สามารถทำงานผ่าน NAT ได้

5. SIP Protocol

การให้บริการ VoIP นั้นโดยปกติแล้วนิยมใช้โพรโตคอลซิปสำหรับการเริ่มต้นการติดต่อเพื่อสร้าง session ของการติดต่อขึ้นมาโดยจะต้องมีกระบวนการ register เป็นสมาชิกของ SIP Server ก่อนจึงจะสามารถโทรไปหาผู้ใช้ที่มีชื่ออยู่ในระบบเดียวกันหรือต่างกันได้ โดย Client ฝั่งผู้ใช้จะส่ง URI ซึ่งประกอบไปด้วยข้อมูลสำคัญคือเช่น ชื่อผู้ใช้ต้นทาง และ ชื่อผู้ใช้ปลายทาง ดังภาพที่ 5 SIP Header

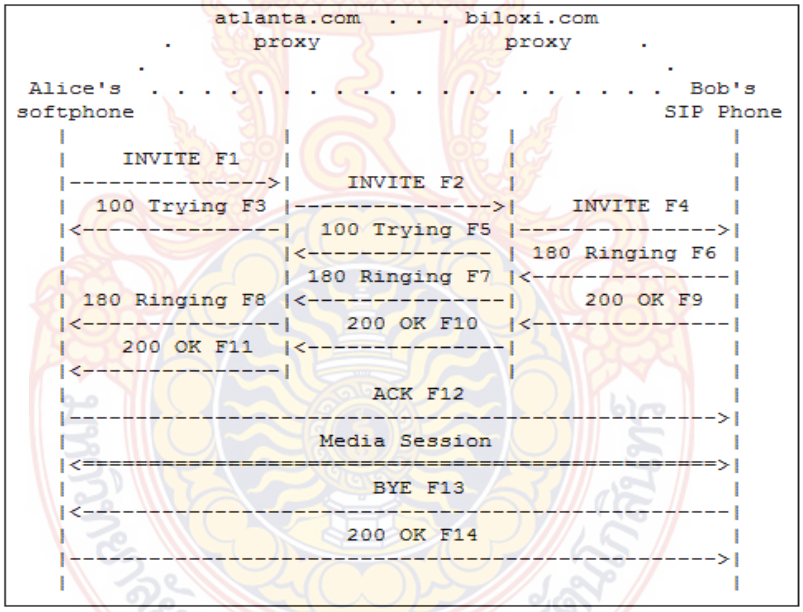
ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

(Alice's SDP not shown)
```

ภาพที่ 5 SIP Header[2]

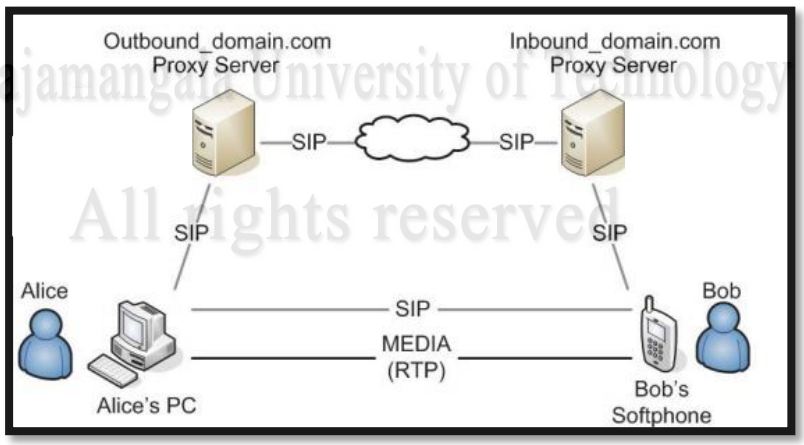
นอกจากนี้ SIP URI ยังประกอบไปด้วยส่วนต่างๆ ที่จำเป็นในการเชื่อมต่อระหว่างผู้ส่งและผู้รับซึ่งการสร้างช่องทางการติดต่อสามารถแสดงได้ดังภาพที่ 6 แสดงการสร้าง SIP Session ระหว่าง Alice กับ Bob ซึ่งประกอบไปด้วย ชื่อผู้ใช้งาน, ชื่อโดเมน, เวอร์ชั่นของ SIP Protocol, Protocol ที่ใช้งานซึ่งในภาพที่ 5 ระบุเป็น UDP Protocol นอกจากนี้ยังมีข้อมูลระบุว่าใครคือผู้โทร โทรหาใคร และ Packet นี้เป็น INVATE มีขนาดความยาวของข้อมูล 142 ไบต์



ภาพที่ 6 แสดงการสร้าง SIP Session ระหว่าง Alice กับ Bob[2]

โดยการติดต่อระหว่างผู้โทรและผู้รับสายโดยปกติสามารถแสดงได้ดังภาพที่ 7 โครงสร้างของระบบ ซึ่งจะเห็นว่ามี SIP Proxy ทำหน้าที่เป็น Server ให้บริการทั้งฝั่งผู้รับและผู้โทร

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved



ภาพที่ 7 โครงสร้างของระบบ[1]

ทั้งนี้จากภาพที่ 7 โครงสร้างของระบบ จะพบว่าเมื่อ Bob ต้องการโทรไปหา Alice ก่อนอื่นทั้งสองคนต้องอยู่ในระบบและเข้าระบบด้วย Softphone หรือมี IP Phone ทั้งคู่ จากนั้น Bob จะต้องระบุเบอร์หรือชื่อผู้ใช้ปลายทาง ซึ่งหาก SIP Server ทางฝั่ง Bob ไม่มีชื่อผู้ใช้ดังกล่าวที่ Bob ต้องการติดต่อด้วย Sip Server ก็จะติดต่อไปยัง SIP server ภายนอกซึ่งจากภาพก็คือ SIP Server ที่ Alice เป็นสมาชิกอยู่นั้นเอง

6. ภาษา Perl

ภาษาเพิร์ล (Perl) ย่อมาจาก Practical Extraction and Report Language เป็นภาษาโปรแกรมแบบไดนามิก พัฒนาโดยนายแลร์รี วอลล์ (Larry Wall) ในปี ค.ศ. 1987 เพื่อใช้งานกับระบบปฏิบัติการยูนิกซ์

ภาษาเพิร์ล นั้นถูกออกแบบมาให้ใช้งานได้ง่าย โครงสร้างของภาษาจึงไม่ซับซ้อน มีลักษณะคล้ายกับภาษาซี นอกจากนี้เพิร์ลยังได้แนวคิดบางอย่างมาจากเชลล์สคริปต์, ภาษา AWK, sed และ Lisp โครงสร้างของภาษา ดังตัวอย่างการเขียนโปรแกรม Hello World ด้วยภาษาเพิร์ลดังนี้

```
#!/usr/bin/perl
print "Hello, world!\n";   # '\n' is a 'newline'
```

บรรทัดแรกเป็นการประกาศให้ระบบปฏิบัติการค้นหาตัวแปลภาษาเพิร์ลตามตำแหน่งที่ระบุ ส่วนบรรทัดที่สองเป็นการพิมพ์ข้อความ (หรือสตริง) ว่า "Hello, world!" และสัญลักษณ์ในการขึ้นบรรทัดใหม่ออกมา ตามด้วยความเห็นหรือคอมเมนต์ว่า '\n' is a 'newline' ในบรรทัดเดียวกัน สำหรับรุ่น 5.10 สามารถเขียนได้อีกแบบว่า

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

```
#!/usr/bin/perl
say "Hello, world!";
```

Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

ภาษาเพิร์ลมีตัวแปรอยู่ 4 ชนิด ได้แก่

1. สเกลาร์สามารถเก็บข้อมูลได้ 1 อย่างอาจจะเป็น ตัวเลข,สตริงหรือรีเฟอเรนซ์ก็ได้
2. อาเรย์ เป็นเสมือนกลุ่มของสเกลาร์ที่ถูกเรียงไว้
3. แฮช หรืออีกชื่อหนึ่งคือแถวลำดับแบบจับคู่ เป็นเสมือนตู้ล็อกเกอร์สำหรับเก็บสเกลาร์ กุญแจที่จะใช้ไขตู้ล็อกเกอร์จะเรียกว่า keys

4. ไฟล์แฮนเดิล เป็นตัวแปรที่ใช้สำหรับ I/O โดยเฉพาะ อาจจะใช้สำหรับรับการสั่งงานจากผู้ใช้ผ่านทาง Standard Input หรือใช้สำหรับแสดงผลออกทาง Standard Output

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

บทที่ 3
ระเบียบวิธีการวิจัย

งานวิจัยนี้ได้ออกแบบระบบเพื่อให้มีความสามารถตรวจสอบผู้โทรได้โดยผู้โทรนั้นเราจะสามารถทราบได้ว่าเป็นใครจาก SIP URI ซึ่งระบบจะถอดออกมาจาก SIP Packet แล้วจะนำไปตรวจสอบกับฐานข้อมูล Blacklist, Whitelist และ Graylist เพื่อยืนยันว่าเป็น SPIT หรือ ผู้โทรปกติ

1. การพัฒนาระบบ

ในงานวิจัยนี้ระบบจะมี 2 ส่วนคือ

1.1 ส่วนของชุดโปรแกรมที่สนับสนุนการทำงานของ VoIP Gateway ตามปกติโดยใช้โปรแกรม Asterisk ในการให้บริการ

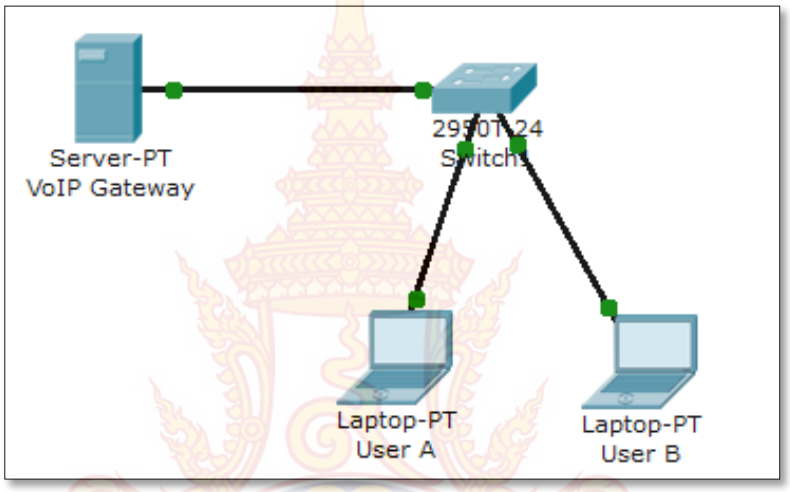
1.2 ส่วนของโปรแกรมที่พัฒนาเพิ่มเข้ามาให้ทำงานร่วมกันโดยทำหน้าที่คอยดักจับข้อมูลการโทรจาก A ไปยัง B เพื่อนำ SIP URI มาตรวจสอบกับ Blacklist, Whitelist และ Graylist เพื่อตรวจสอบและป้องกันการโทรที่เป็น SPIT ไม่ให้โทรไปยังผู้ใช้ปกติ

2. การออกแบบระบบ

2.1 การจำลองเครือข่ายสำหรับการทดสอบ

ในส่วนของการติดตั้งระบบเข้ากับระบบเครือข่ายนั้น สำหรับในงานวิจัยนี้ได้จำลองการเชื่อมต่อระหว่าง ผู้โทร A และ B หรือมากกว่ากับ VoIP Gateway ดังแสดงในภาพที่ 8 Network Diagram

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved



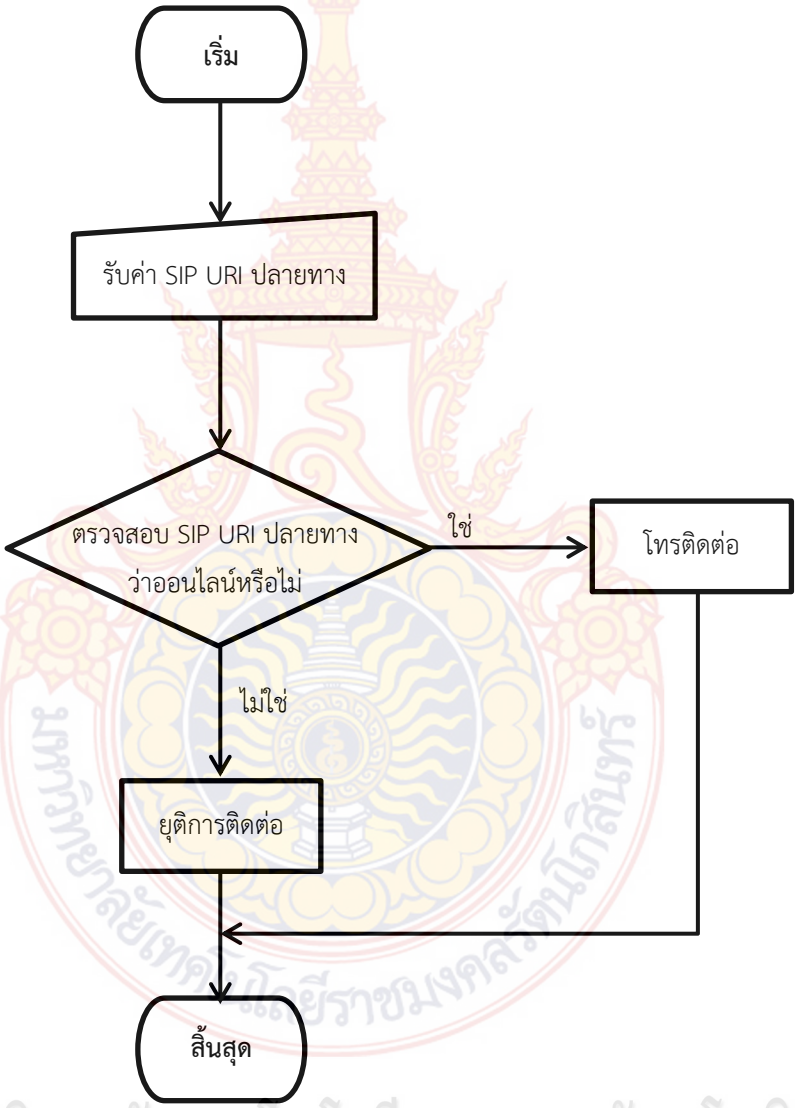
ภาพที่ 8 Network Diagram

2.2 การพัฒนาระบบ

2.2.1 การทำงานเดิมของ VoIP Gateway โดยใช้โปรแกรม Asterisk ซึ่งการทำงานเดิมนั้นมีขั้นตอนดังภาพที่ 9 Flowchart การทำงานของ VoIP Gateway แบบเดิม

จาก Flowchart ในภาพที่ 9 กระบวนการทำงานปกตินั้นจะเริ่มต้นตั้งแต่ผู้โทรระบุ SIP URI ปลายทางจากนั้นระบบจะทำการตรวจสอบว่า SIP URI ปลายทางนั้น Online อยู่หรือไม่หากใช่ก็จะทำการส้รางการติดต่อระหว่างผู้โทรไปหาปลายทางทันที แต่ถ้าไม่ใช่นั้นหมายถึง SIP URI ดังกล่าวมิได้ Online คือไม่ได้เชื่อมต่อกับระบบก็จะยุติการเชื่อมต่อทันที

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved



ภาพที่ 9 Flowchart การทำงานของ VoIP Gateway แบบเดิม

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

Copyright © by Rajamangala University of Technology Rattanakosin

2.2.2 การทำงานที่ปรับปรุงโดยการเพิ่มโปรแกรมในส่วนของการตรวจสอบสถานะของ SIP URI ว่าเป็น SPIT หรือไม่โดยการตรวจสอบการ Whitelist, Blacklist และ Graylist สามารถแสดงการทำงานดังภาพที่ 10 Flowchart การทำงานของ VoIP Gateway โดยเพิ่มโปรแกรมตรวจสอบ

All rights reserved

ภาพที่ 10 Flowchart การทำงานของ VoIP Gateway โดยเพิ่มโปรแกรมตรวจสอบ

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

ดังในแสดงใน Flowchart ในภาพที่ 10 แสดงส่วนของโปรแกรมที่ทำการปรับปรุงและพัฒนาเพิ่มเติมให้ทำงานร่วมกับการทำงานของ VoIP Gateway เดิม โดยเมื่อมีการโทรเกิดขึ้นระบบจะทำการบันทึก SIP URI ไว้ใน Graylist เพื่อใช้เป็นข้อมูลในการเทียบเทียบความถี่ในการโทรว่าเกินกว่าเกณฑ์ที่กำหดนหรือไม่ในภายหลัง เมื่อบันทึกข้อมูลเสร็จแล้วก็จะเป็นการตรวจสอบว่า SIP URI ดังกว่าเคยมีการติดต่อจากผู้รับไปหรือไม่โดยจะนำ SIPURI ของผู้ที่โทรเข้ามาเรียกว่า Caller ไปตรวจสอบกับข้อมูลของผู้รับในส่วนของข้อมูลผู้โทรใน Calllog หากพบข้อมูลของ Caller อยู่ใน Calllog ตรงกับ Callee ที่เคยมีการติดต่อไปจาก ผู้ใช้รายนี้ซึ่งคือผู้รับในปัจจุบันก็จะทำการบันทึกไว้ใน Whitelist และจะตรวจสอบต่อไปว่ามีอยู่ใน Whitelist หรือไม่หากพบก็จะเชื่อมต่อการโทรให้ แต่หากไม่พบก็จะทำการตรวจสอบต่อไปยัง Blacklist ซึ่งหากพบก็จะยุติการโทรทันที แต่หากไม่พบทั้งสองฐานข้อมูลก็จะเข้าสู่กระบวนการตรวจสอบว่ามีความพยายามโทรเกินกว่าเกณฑ์หรือไม่ถ้าไม่ใช่ก็จะโทรติดต่อทันที แต่หากเกินกว่าเกณฑ์ที่กำหนดระบบจะยุติการโทรและทำการบันทึก SIP URI ดังกล่าวใน Blacklist จากนั้นจะลบข้อมูล SIP URI ออกจาก Graylist และสิ้นสุดการทำงาน

2.3 การติดตั้งโปรแกรมที่จำเป็น

เนื่องจากงานวิจัยนี้เป็นการพัฒนาโปรแกรมเพิ่มเติมเข้าไปทำงานร่วมกับบริการ VoIP เดิมที่มีอยู่แล้วโดยเลือกที่จะพัฒนาชุดโปรแกรมเพิ่มเติมให้ทำงานร่วมกับโปรแกรม Asterisk ซึ่งมีความสามารถเป็ฯ VoIP Gateway ที่สามารถจัดการคู่สายการโทร และมีระบบจัดการผู้ใช้งาน โดยในส่วนแรกเริ่มนั้นผู้วิจัยจะทำการติดตั้งชุดโปรแกรม Asterisk บนระบบปฏิบัติการ Linux โดยใช้ Centos Linux เวอร์ชั่น 5.4 ขึ้นไป ซึ่งส่วนประกอบที่จำเป็นของงานวิจัยมีดังนี้

1. ระบบปฏิบัติการ CentOS Linux
2. ชุดโปรแกรม Asterisk
3. โปรแกรมฐานข้อมูล Mysql
4. โปรแกรมแปลภาษา Perl
5. โปรแกรมเสริม Asterisl-Perl
6. โปรแกรม Net-DNSม Net-IP
7. โปรแกรมจัดการฐานข้อมูล phpMyadmin

เมื่อได้ติดตั้งโปรแกรมที่จำเป็นทั้งหมดตามที่กล่าวไว้ข้างต้นแล้วผู้วิจัยจึงพัฒนาโปรแกรมด้วยภาษา Perl ร่วมกับการปรับปรุงแผนการโทร(DialPlan)ของ Asterisk โดยการแก้ไขไฟล์ที่ชื่อว่า Extension.conf โดยมีที่อยู่ของไฟล์คือ /etc/asterisk/extension.conf

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

2.4 การออกแบบฐานข้อมูล

สำหรับฐานข้อมูลที่ใช้ในงานวิจัยนี้คือ Mysql โดยจะประกอบด้วยตารางทั้งหมด 4 ตาราง คือ Calllog, Whitelist(wl), Graylist(gl) และ Blacklist(bl)

caller	callee	datetime
600@172.22.32.46	601@172.22.32.46	2014-08-27 12:08:17

ภาพที่ 11 ตาราง Calllog

IP	datetime
192.168.157.1	2014-07-13 10:39:24
192.168.157.1	2014-07-13 10:39:22
192.168.157.1	2014-07-13 10:39:10

ภาพที่ 12 ตาราง Graylist(gl)

IP	date
192.168.157.1	2014-07-13

ภาพที่ 13 ตาราง Whitelist(wl) และ Blacklist(bl)

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

Copyright © by Rajamangala University of Technology Rattanakosin

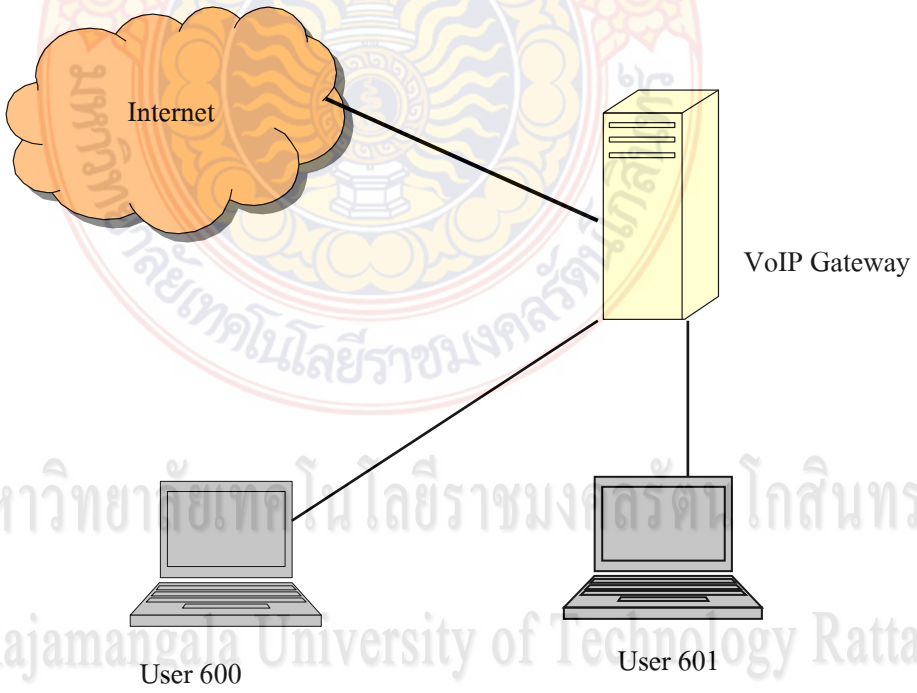
All rights reserved

บทที่ 4
ผลการวิจัย

1. ผลการทดสอบการทำงานของระบบ

ในการทดสอบนั้นจะแบ่งเป็นการโทรปกติ และการโทรที่ไม่ปกติซึ่งจำลองการที่เกิดจาก SPIT เพื่อทดสอบการตรวจจับและปิดกั้นการโทรที่มีลักษณะเป็น SPIT

1.1 การทดสอบการโทรปกติ โดยจะทดสอบการโทรจากหมายเลข 600 ไปหาผู้ใช้หมายเลข 601 โดยจำลองการโทรโดยผู้ใช้งานปกติ และมีการรับสายและสนทนาปกติโดยใช้ Softphone x-lite ซึ่งติดตั้งใช้งานบนเครื่องคอมพิวเตอร์และ Zoiper ซึ่งติดตั้งบนสมาร์ทโฟน Android



ภาพที่ 14 การเชื่อมต่ออุปกรณ์สำหรับการทดสอบการโทรปกติ

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

โดยผู้วิจัยทำการ Online ชื่อผู้ใช้ทั้งสองทั้งบนคอมพิวเตอร์และบนสมาร์ทโฟนซึ่งเมื่อการพิสูจน์ตัวตนสำเร็จระบบก็จะแสดงสถานะเพื่อให้ทราบดังแสดงในภาพที่ 15 สถานะการเชื่อมต่อซึ่งจากรูปแสดงให้เห็นว่าการพิสูจน์ตัวตนสมบูรณ์และสถานะทั้งสองชื่อผู้ใช้ทั้ง 600 และ 601 จะอยู่ใน

สถานะ Online พร้อมที่จะติดต่อไปยังผู้ใช้คนอื่นๆ ซึ่งการทดลองในขั้นตอนนี้จะโทรติดต่อจากเบอร์ 600 ไปยังเบอร์ 601 ระบบจะแสดงสถานะการติดต่อดังภาพที่ 16

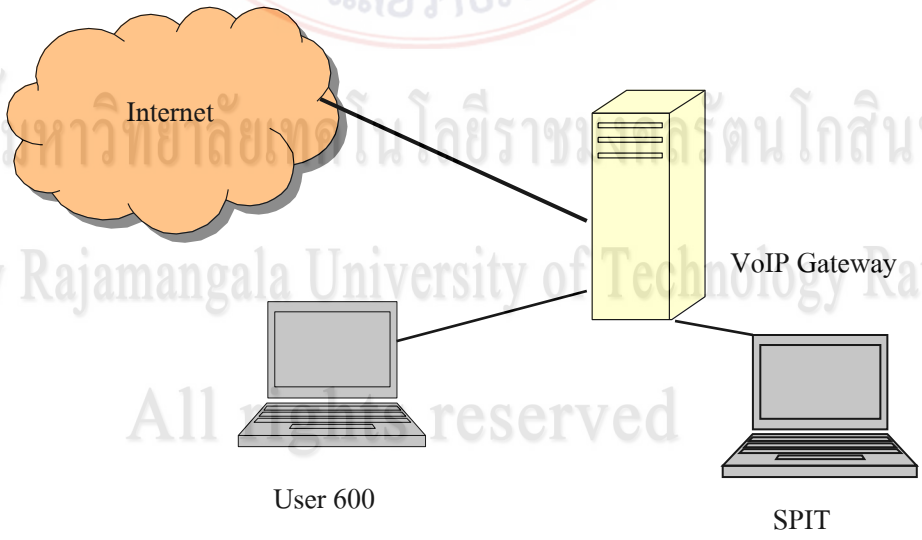
```
localhost*CLI>
    -- Registered SIP '600' at 172.22.32.35 port 64880
    -- Saved useragent "X-Lite 4.7.0 73589-270c1c94-W6.1" for peer 600
    -- Registered SIP '601' at 203.158.222.50 port 46853
    -- Saved useragent "Zoiper r26525" for peer 601
localhost*CLI>
```

ภาพที่ 15 สถานะการเชื่อมต่อ

```
localhost*CLI>
    -- Executing [601@demo:1] Dial("SIP/600-0000000e", "SIP/601") in new stack
    -- Called 601
    -- SIP/601-0000000f is ringing
    -- SIP/601-0000000f answered SIP/600-0000000e
    -- Packet2Packet bridging SIP/600-0000000e and SIP/601-0000000f
```

ภาพที่ 16 แสดงสถานะการติดต่อจากเบอร์ 600 ไปหาเบอร์ 601

1.2 การทดสอบการโทรที่เป็น SPIT ซึ่งจำลองการโทรที่เป็น SPIT ในกรณีเช่นโทรไปหาผู้ใช้ A เมื่อผู้ใช้ A วางสายหรือตัดสายทิ้งก็โทรไปหาผู้ใช้ B ต่อในทันทีและเมื่อผู้ใช้ B ตัดสายหรือวางสายก็จะโทรไปยังผู้ใช้ถัดไปทันทีอย่างต่อเนื่องในเวลาที่ไล่เลี่ยกัน



ภาพที่ 17 การเชื่อมต่ออุปกรณ์สำหรับการทดสอบการโทรที่เป็น SPIT

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

การทดลองเริ่มจากออนไลน์ผู้ใช้หมายเลข 600 ให้เป็นผู้ใช้ปกติและหมายเลข 666 เป็นหมายเลขของ SPIT

```
localhost*CLI>
    -- Registered SIP '666' at 203.158.222.50 port 64088
    -- Saved useragent "Zoiper r26525" for peer 666
    -- Registered SIP '600' at 172.22.32.35 port 65158
    -- Saved useragent "X-Lite 4.7.0 73589-270c1c94-W6.1" for peer 600
localhost*CLI>
```

ภาพที่ 18 สถานะการเชื่อมต่อผู้ใช้ปกติและ SPIT

จากการทดลองพบว่าเมื่อมีการโทรจากผู้ใช้งานปกติดังแสดงในภาพที่ 14 ระบบจะปล่อยให้การโทรนั้นเกิดขึ้นตามปกติโดยไม่มีการปิดกันแต่อย่างใด เนื่องจากการโทรที่เป็นปกตินั้นผู้ใช้มิได้โทรไปยังปลายทางในอัตราที่บ่อยเกินไป ในทางกลับกันการทดสอบการโทรที่เกิดจาก SPIT ดังแสดงในภาพที่ 17 นั้นระบบจะตรวจพบความผิดปกติเมื่อ SPIT พยายามโทรไปยังผู้ใช้ปกติถี่เกินไปในช่วงระยะเวลาที่ใกล้เคียงกันเช่นในเวลา 30 นาที SPIT อาจจะพยายามโทรติดต่อไปยังผู้ใช้ถึง 15-25 ครั้ง ซึ่งขึ้นอยู่กับว่าผู้ใช้งานรับสายและฟังข้อความเสียงหรือไม่สำหรับ SPIT เองอาจจะใช้วิธีการโทรไปยังเหยื่อโดยเรียงตามลำดับรายการข้อมูลเบอร์ติดต่อที่ได้ถูกสร้างไว้ก่อนแล้วหรือโดยการสุ่มจากรายการเบอร์ติดต่อก็ได้

2. ความพึงพอใจต่อระบบ

ผู้วิจัยได้สอบถามความพึงพอใจต่อระบบกับผู้ใช้โดยการเลือกสุ่มนักศึกษา อาจารย์ เจ้าหน้าที่และบุคคลทั่วไปจำนวน 30 คนซึ่งได้ผลดังตารางที่ 1 แสดงถึงจำนวนร้อยละและค่าเฉลี่ยความพึงพอใจต่อระบบจำกัดและป้องกันสายไม่พึงประสงค์ของการใช้บริการโทรศัพท์ผ่านอินเตอร์เน็ตโดยการระบุและปิดกั้น URI ของโพรโตคอล SIP โดยค่าความพึงพอใจ จะอยู่ในระดับ 5 คือ ดีมาก ระดับ 4 คือ ดี และ มีค่าเฉลี่ย $\overline{X}$ = 4.88 และค่า S.D = 0.32 ทั้งนี้ความพึงพอใจที่มีค่เฉลี่ย $\overline{X}$ สูงสุดคือ การตรวจสอบเพื่อระบุ SPIT = 4.93 รองมาคือ ประโยชน์เมื่อนำไปใช้, การป้องกันการทำงานของ SPIT และ ประโยชน์ที่ได้จากระบบ ซึ่งมีค่าเท่ากันคือ 4.90 ส่วน การทำงานของระบบโดยรวม มีค่าต่ำสุดคือ 4.77

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

ตารางที่ 1 ความพึงพอใจต่อระบบจำกัดและป้องกันสายไม่พึงประสงค์ของการใช้บริการโทรศัพท์ผ่านอินเตอร์เน็ตโดยการระบุและปิดกั้น URI ของโพรโตคอล SIP

ความพึงพอใจต่อการให้บริการ	คะแนน(5 ดีมาก,4 ดี,3 ปานกลาง,2 พอใช้, 1 ปรับปรุง)					$\overline{X}$	S.D
	5	4	3	2	1		
การให้บริการระบบการเรียนรู้ด้วยตนเองของนักศึกษาโดยใช้สื่อประสมบนเว็บ							
1. ประโยชน์เมื่อนำไปใช้	27 (90.00)	3 (10.00)	-	-	-	4.90	0.31
2. การทำงานของระบบโดยรวม	23 (76.67)	7 (23.33)	-	-	-	4.77	0.43
3. การตรวจสอบเพื่อระบุ SPIT	28 (93.33)	2 (6.67)	-	-	-	4.93	0.25
4. การป้องกันการทำงานของ SPIT	27 (90.00)	3 (10.00)	-	-	-	4.90	0.31
5. ประโยชน์ที่ได้จากระบบ	27 (90.00)	3 (10.00)	-	-	-	4.90	0.31
รวม						4.88	0.32

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

บทที่ 5
สรุปผล อภิปรายผลและข้อเสนอแนะ

1. สรุปผลการวิจัย

จากการศึกษาพบว่าการตรวจสอบโดยใช้โปรแกรมที่พัฒนาขึ้นมาร่วมกับ Asterisk ซึ่งเป็น VoIP Gateway นั้นสามารถตรวจสอบ และป้องกัน การโทรของสายที่ไม่พึงประสงค์ไปยังผู้ใช้งานปกติได้ ทั้งนี้เนื่องจาก VoIP Gateway ต้องดึง SIP URI ไปตรวจสอบด้วยโปรแกรมซึ่งต้องมีการติดต่อกับฐานข้อมูลด้วย ดังนั้นจึงต้องเสียเวลาในการตรวจสอบ แต่ก็ใช้เวลาเพียงเล็กน้อยเท่านั้น

ค่าความพึงพอใจ จะอยู่ในระดับ 5 คือ ดีมาก และ ระดับ 4 คือ ดี โดยมีค่าเฉลี่ย $\overline{X}$ = 4.88 และค่า S.D = 0.32 ทั้งนี้ความพึงพอใจที่มีค่าเฉลี่ย $\overline{X}$ สูงสุดคือ การตรวจสอบเพื่อระบุ SPIT = 4.93 รองมาคือ ประโยชน์เมื่อนำไปใช้, การป้องกันการทำงานของ SPIT และ ประโยชน์ที่ได้จากระบบ ซึ่งมีค่าเท่ากันคือ 4.90 ส่วน การทำงานของระบบโดยรวม มีค่าต่ำสุดคือ 4.77

2. การอภิปรายผล

การศึกษาและทดลองพบว่าระบบสามารถตรวจสอบได้ว่าการโทรใดเป็นการโทรที่ได้รับความไว้ใจจากผู้ใช้โดยการบันทึกด้วยตัวผู้ใช้เองในรายการ Whitelist ทำให้โทรไปยังปลายทางได้ปกติ

สำหรับการโทรที่ถูกบันทึกในรายการ Blacklist ไปแล้วนั้น ก็จะถูกปิดกัน ไม่ให้สามารถโทรไปยังหมายเลขปลายทางใดๆ ได้จนกว่าจะมีการนำหมายเลขดังกล่าวออกจากรายการ Blacklist ระบบสามารถตรวจสอบการโทรที่ผิดปกติที่เป็น SPIT ได้และเมื่อตรวจพบแล้วจะทำการปิดกันการโทรโดยการยกเลิกสายโทรนั้นและบันทึกหมายเลขดังกล่าวในรายการ Blacklist

จากการทดลองพบว่าเมื่อพยายามโทรเพื่อจำลองการทำงานของ SPIT จนเกินกว่าค่าที่กำหนดในคาบเวลาที่กำหนดจะทำให้หมายเลขดังกล่าวถูกตัดสายทันทีที่โทรออกไป ซึ่งเกิดจากการที่ระบบบันทึกหมายเลขดังกล่าวว่าเป็น SPIT ในรายการ Blacklist จึงช่วยให้ผู้ให้ VoIP Gateway สามารถคัดกรอง SPIT ออกจากผู้ใช้งานปกติได้

3. ข้อเสนอแนะ

สำหรับงานวิจัยนี้ได้ใช้โปรแกรมที่พัฒนาจากภาษา Perl มาเป็นส่วนสำคัญในการตรวจสอบและสกัดกั้นการโทรที่อาจจะเป็น SPIT ซึ่งจะทำให้เกิดการเสียเวลาในการทำงานของโปรแกรมที่ทำ

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

หน้าที่ตรวจสอบดังนั้นในการพัฒนาต่อไปจึงต้องหาโปรแกรมที่มีการทำงานที่รวดเร็วกว่าหากว่ามี แต่ก็ต้องสามารถทำงานได้กับ Linux Asterisk ด้วย อีกประเด็นคือเนื่องจากมีการใช่งานระบบฐานข้อมูล ดังนั้นจึงเป็นช่องโหว่ที่อาจถูกโจมตีได้ ซึ่งหากนำระบบดังกล่าวไปใช้งานจริงจึงควรสร้างระบบป้องกันฐานข้อมูลและปิดช่องโหว่ให้ดีเพื่อป้องกันการโจมตีด้านฐานข้อมูล

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

บรรณานุกรม

1. Alexander J. Johansen and Woraphon Lilakiatsakun, **“A VOIP anti-Spam System based on Modular Mechanism Design”**, 2010

2. IETF “SIP: Session Initiation Protocol”2002, สามารถเข้าถึงข้อมูลได้จาก http://www.ietf.org/rfc/rfc3261.txt

3. Dr. Andreas U. Schmidt, Nicolai Kuntze **“Spam over Internet telephony and how to deal with it”**

4. About Asterisk. Internet: http://www.asterisk.org/support/about, [Dec. 10, 2008]

5. M. Spencer, B. Capouch, E. Guy, F. Miller, K. Shumard, **“IAX: Inter-Asterisk eXchange Version 2”**. October 6, 2008

6. Spamhaus Block List. สามารถเขาถึงข้อมูลได้จาก : http://www.spamhaus.org/whitepapers/dnsbl_function.html

7. การสื่อสารทางเสียงผ่านเครือข่าย IP.สามารถเข้าถึงข้อมูลได้จาก : http://www.ku.ac.th/magazine_online/voip.html

8. การโทรศัพท์ผ่านเครือข่ายอินเตอร์เน็ต(VoIP). สามารถเข้าถึงข้อมูลได้จาก : http://voip.forthai.com/voip/

9. บริการโทรศัพท์ผ่านอินเตอร์เน็ต. สามารถเข้าถึงข้อมูลได้จาก : http://www.vcharkarn.com/blog/35869/5746

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

Copyright © by Rajamangala University of Technology Rattanakosin

All rights reserved

ประวัติผู้วิจัย

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

ประวัติผู้วิจัย

1. ชื่อ-สกุล นายศิวะพร วิวัฒน์ภิญโญ

2. ตำแหน่งปัจจุบัน อาจารย์

3. หน่วยงานที่สามารถติดต่อได้

สาขาวิชาเทคโนโลยีวิศวกรรมคอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ วิทยาเขตวังไกลกังวล ต.หัวหิน อ.หัวหิน
จ.ประจวบคีรีขันธ์ รหัสไปรษณีย์ 77110
หมายเลขโทรศัพท์ที่ทำงาน 032-618500 ต่อ 4032 โทรสาร 032-618570
โทรศัพท์มือถือ 0858197154
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail) siwaphon.viw@rmutr.ac.th

4. ประวัติการศึกษา

ปริญญาโท มหาวิทยาลัยเทคโนโลยีมหานคร วิทยาศาสตรมหาบัณฑิต เทคโนโลยีสารสนเทศ (วิศวกรรมเครือข่าย), “พ.ศ.2554”

ปริญญาตรี สถาบันเทคโนโลยีราชมงคลรัตนโกสินทร์ อุตสาหกรรมศาสตร์บัณฑิต เทคโนโลยีคอมพิวเตอร์, “พ.ศ.2547”

5. สาขาวิชาการที่มีความชำนาญพิเศษ

เทคโนโลยีสารสนเทศ, วิศวกรรมเครือข่าย, เทคโนโลยีคอมพิวเตอร์

6. ประสบการณ์ที่เกี่ยวข้องกับการบริหารงานวิจัย

6.1 พัฒนาระบบการเรียนรู้ด้วยตนเองของนักศึกษาโดยใช้สื่อประสมบนเว็บ ปีงบประมาณ 2556 สนุบสนุนโดยเงินงบประมาณแผนดิน มทร.รัตนโกสินทร์

6.2 ความไม่ปลอดภัยของการใช้บริการโทรศัพท์ผ่านอินเตอร์เน็ต กรณีศึกษาการดักฟัง ปีงบประมาณ 2557 สนุบสนุนโดยเงินงบประมาณแผนดิน มทร.รัตนโกสินทร์ สถานภาพหัวหน้าโครงการวิจัย

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

6.3 การจำกัดและป้องกันสายไม่พึงประสงค์ของการใช้บริการโทรศัพท์ผ่านอินเตอร์เน็ตโดยการการระบุและปิดกั้น URI ของโพรโตคอล SIP

ปีงบประมาณ 2557 สนุบสนุนโดยเงินงบประมาณแผนดิน มทร.รัตนโกสินทร์

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

Copyright © by Rajamangala University of Technology Rattanakosin

All rights reserved

ประวัติผู้วิจัย

1. ชื่อ-สกุล นายพรประสิทธิ์ บุญทอง

2. ตำแหน่งปัจจุบัน อาจารย์ 7

3. หน่วยงานที่สามารถติดต่อได้

สาขาวิชาเทคโนโลยีวิศวกรรมคอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ วิทยาเขตวังไกลกังวล ต.หัวหิน อ.หัวหิน
จ.ประจวบคีรีขันธ์ รหัสไปรษณีย์ 77110
หมายเลขโทรศัพท์ที่ทำงาน 032-618500 ต่อ 4035 โทรสาร 032-618570
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail) pornprasit@idt.rmutr.ac.th

4. ประวัติการศึกษา

ปริญญาโท สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
วิศวกรรมศาสตร์มหาบัณฑิต วิศวกรรมคอมพิวเตอร์,
ปริญญาตรี สถาบันเทคโนโลยีราชมงคล วิศวกรรมศาสตร์บัณฑิต
วิศวกรรมคอมพิวเตอร์,

5. สาขาวิชาการที่มีความชำนาญพิเศษ

วิศวกรรมคอมพิวเตอร์

6. ประสบการณ์ที่เกี่ยวข้องกับการบริหารงานวิจัย

-

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

ประวัติผู้วิจัย

1. ชื่อ-สกุล นางสาวศิริเรือง พัฒน์ช่วย

2. ตำแหน่งปัจจุบัน อาจารย์

3. หน่วยงานที่สามารถติดต่อได้

สาขาวิชาเทคโนโลยีวิศวกรรมคอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ วิทยาเขตวังไกลกังวล ต.หัวหิน อ.หัวหิน
จ.ประจวบคีรีขันธ์ รหัสไปรษณีย์ 77110
หมายเลขโทรศัพท์ที่ทำงาน 032-618500 ต่อ 4032 โทรสาร 032-618570
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail) siriruang.ph@hotmail.com

4. ประวัติการศึกษา

ปริญญาโท มหาวิทยาลัยธุรกิจบัณฑิตย์ วิทยาศาสตรมหาบัณฑิต
เทคโนโลยีคอมพิวเตอร์และการสื่อสาร “พ.ศ.2552”
ปริญญาตรี มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ บริหารธุรกิจบัณฑิต
ระบบสารสนเทศ, “พ.ศ.2549”

5. สาขาวิชาการที่มีความชำนาญพิเศษ

วิศวกรรมซอฟต์แวร์, การพัฒนาซอฟต์แวร์ระดับองค์การ, ระบบฐานข้อมูล

6. ประสบการณ์ที่เกี่ยวข้องกับการบริหารงานวิจัย

-

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
All rights reserved

ประวัติผู้วิจัย

1. **ชื่อ-สกุล** นายอาทิตย์ อยู่เย็น

2. **ตำแหน่งปัจจุบัน** อาจารย์

3. **หน่วยงานที่สามารถติดต่อได้**

สาขาวิชาเทคโนโลยีวิศวกรรมคอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ วิทยาเขตวังไกลกังวล ต.หัวหิน อ.หัวหิน
จ.ประจวบคีรีขันธ์ รหัสไปรษณีย์ 77110
หมายเลขโทรศัพท์ที่ทำงาน 032-618500 ต่อ 4032 โทรสาร 032-618570
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail) thit19@hotmail.com

4. ประวัติการศึกษา

ปริญญาโท มหาวิทยาลัยเทคโนโลยีมหานคร วิทยาศาสตรมหาบัณฑิต
เทคโนโลยีสารสนเทศ “พ.ศ.2550”
ปริญญาตรี สถาบันเทคโนโลยีราชมงคล วข.วังไกลกังวล อุตสาหกรรมศาสตร์บัณฑิต
เทคโนโลยีคอมพิวเตอร์, “พ.ศ.2547”

5. สาขาวิชาการที่มีความชำนาญพิเศษ

ระบบควบคุมโรงงานอุตสาหกรรม, ระบบคอนโทรลเลอร์, อิเล็กทรอนิกส์, ระบบสานสนเทศและการโปรแกรมมิ้ง

6. ประสบการณ์ที่เกี่ยวข้องกับการบริหารงานวิจัย

ลิขสิทธิ์มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
Copyright © by Rajamangala University of Technology Rattanakosin
- All rights reserved