การประเมินผลกระทบจากการโจมตีแบบการปฏิเสธการให้บริการบนระบบโทรศัพท์ผ่านอินเทอร์เน็ต

DENIAL OF SERVICE ATTACH IMPACT ASSESSMENT ON A VOICE OVER INTERNET PROTOCOL SYSTEM

ภูวิช แก้วหาญ[1]

ชัยพร เขมะภาตะพันธ์[2]

บทคัดย่อ

งานวิจัยนี้มีจุดประสงค์ในการศึกษา ประเมินผลกระทบของช่องโหว่ของระบบโทรศัพท์ผ่านอินเตอร์เน็ต(IPPBX SERVER:IPPBX) จากการคุกคามแบบการปฏิเสธการให้บริการ(Denial of Service: Dos) โดยใช้โปรแกรมทดสอบการโจมตีด้วยการส่งคำสั่งร้องขอการเชื่อมต่อ(SIP INVITE) จำนวนมากไปยัง IPPBX โดยเปรียบเทียบกับกรณีโจมตีผ่านระบบเชื่อมต่อสัญญาณโทรศัพท์ผ่านอินเทอร์เน็ต(SIP PROXY SERVER: SIP PROXY) ที่มีคุณสมบัติโปรแกรมป้องกันการคุกคาม

ผลลัพธ์จากศึกษาแสดงให้เห็นว่า SIP PROXY ที่มีการเปิดใช้งานโมดูล PIKE สามารถตอบสนองต่อการโจมตีได้โดยสามารถหยุดส่งคำสั่ง SIP INIVTE ไปยัง IPPBX เมื่ออัตราการโทรศัพท์ต่อวินาทีอยู่ในระหว่างค่าอัตราการรับคำสั่งต่อวินาทีที่กำหนดบนโมดูล PIKE ในขณะที่ IPPBX ที่ไม่มีระบบป้องกันไม่สามารถจัดการปัญหา การปฏิเสธการให้บริการนี้ได้เลย การป้องกันทำให้ปริมาณการใช้ทรัพยากรของ IPPBX ไม่เพิ่มขึ้นและไม่มีผลกระทบต่อการให้บริการของระบบ มีผลให้ IPPBX สามารถต้านทานต่อการคุกคามแบบ DoS โดยใช้คำสั่งร้องขอการเชื่อมต่อ SIP INIVTE ได้

คำสำคัญ: ระบบโทรศัพท์ผ่านอินเตอร์เน็ต, การปฏิเสธการให้บริการ,ระบบเชื่อมต่อสัญญาณโทรศัพท์ผ่านอินเทอร์เน็ต,คำสั่งร้องขอการเชื่อมต่อ

---

[1] นักศึกษาหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์

[2] ที่ปรึกษาสารนิพนธ์หลัก

ABSTRACT

The purpose of this research to study vulnerability and assessment of the impact of Internet telephone system(IPPBX) from Denial of Service (DoS) method threats. By sending sip invite message as denial of service to IPPBX from attacker server and sending sip invite message through SIP PROXY SERVER (SIP PROXY) which is enable the Pike module to defense Dos threats and testing result will be comparing by performance and resource utilization of the IPPBX for both type of testing.

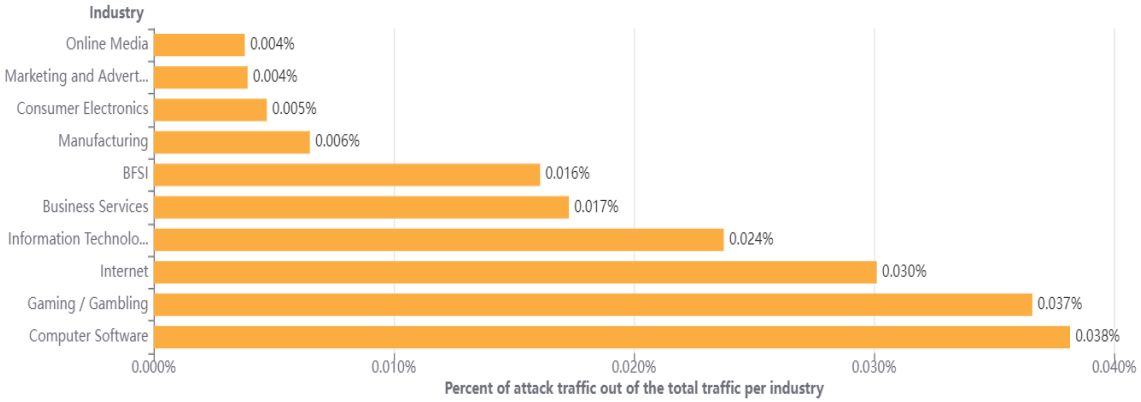
The results of testing show that a SIP PROXY with the Pike module able handle request from attacker. By drop sip invite message to the IPPBX when number of calls per second equal to call per second parameter which is defined in the Pike module. Resource consumption of the IPPBX does not increase and not impact to service of system. As a result, the IPPBX is protected from SIP PROXY which able defense DoS threats.

Keywords: Internet telephone system, Denial of Service, Sip proxy server, SIP INIVTE

1.บทนำ

การที่ในปัจจุบันการสื่อสารข้อมูลต่างๆส่วนมากอาศัยการสื่อสารผ่านอินเทอร์เน็ตความเร็วสูงซึ่งถือได้ว่าเป็นโครงข่ายการสื่อสารข้อมูลที่ได้รับความนิยมทั้งในแง่ความสะดวกรวดเร็วในการติดตั้ง การเข้าถึงได้ง่ายของผู้ให้บริการข้อมูลในแต่ละพื้นที่ ทำให้รูปแบบการบริการข้อมูลบนอินเทอร์เน็ตมีหลากหลายมากขึ้น ซึ่งระบบการสื่อสารโทรศัพท์เช่นเดียวกัน ได้มีการเปลี่ยนแปลงระบบจากการสื่อสัญญาณผ่านโครงข่ายระบบ การสื่อสารแบบแพคเกจสวิตช์(Package switched Telephone) เป็นโทรศัพท์ที่รองรับการเชื่อมต่อผ่านอินเทอร์เน็ต(Voice Over Internet Protocol) ความต้องการเชื่อมต่อระบบโทรศัพท์ผู้ให้บริการหรือสำนักงานที่มีการทำงานจากที่บ้านหรือสถานที่ภายนอกเป็นรูปแบบที่มีความจำเป็นในช่วงที่มีโรคโควิด 2019 ระบาด การปรับรูปแบบการสื่อสารเพื่อไม่ให้มีผลกระทบต่อภาระกิจหรือธุรกิจจะมีความสำคัญอันดับต้นในการดำเนินกิจการให้มีความต่อเนื่อง การปรับเปลี่ยนระบบโทรศัพท์ผ่านอินเทอร์เน็ต จะต้องมีการเตรียมพร้อมในส่วนของเชื่อมต่อสัญญาณให้มีประสิทธิภาพทั้งด้านคุณภาพของการให้บริการและความปลอดภัย

ของระบบโทรศัพท์ทั้งผู้ให้บริการและผู้ใช้บริการ การป้องกันความปลอดภัยของระบบมีความสำคัญอย่างยิ่งดังรายงานการโจมตีระบบเครือข่ายคอมพิวเตอร์ดังภาพที่ 1 นี้



ภาพที่ 1 รายงานการโจมตีแบบ DoS ในไตรมาส 3 ของปี 2564 แยกกลุ่มตามธุรกิจ

ที่มา https://blog.cloudflare.com/ddos-attack-trends-for-2021-q3/

จากภาพที่ 1 การโจมตีโปรแกรมคอมพิวเตอร์และอินเทอร์เน็ต รวมกันแล้วมีอัตราการถูกโจมตีมากที่สุด ซึ่งภัยคุกคามจากสื่อสารผ่านอินเทอร์เน็ตมีหลากหลายรูปแบบที่เป็นภัยต่อระบบการทำงานขององค์กรและผู้ใช้งาน ซึ่งผู้คุกคามจะใช้ประโยชน์จากช่องโหว่ที่มีในระบบสื่อสารข้อมูล เช่นเดียวกันระบบโทรศัพท์ผ่านอินเทอร์เน็ตหลีกเลี่ยงไม่ได้ที่จะโดนคุมคาม โจมตีจากบุคคลประสงค์ร้ายโดยอาศัยช่องโหว่หรือจุดอ่อนของระบบโทรศัพท์ผ่านอินเทอร์เน็ต ซึ่งผลกระทบมีทั้งทางตรงและทางอ้อม ระดับความรุนแรงของภัยดังกล่าวจะแตกต่างกันตามรูปแบบของภัยคุกคาม ดังนั้นการออกแบบหรือพัฒนาระบบโทรศัพท์ผ่านอินเทอร์เน็ต ให้มีความต้านทานภัยต่อคุกคาม หรือหาแนวทางป้องกัน ก็จะทำให้ลดผลกระทบ ในการให้บริการ ความสูญเสียทรัพยากรของระบบและยังคงทำให้ระบบโทรศัพท์ผ่านอินเทอร์เน็ตให้บริการด้วยความเสถียร มีคุณภาพของการให้บริการที่ดี และมีความมั่นคงปลอดภัย น่าเชื่อถือยิ่งขึ้น

2.วัตถุประสงค์ของการวิจัย

2.1. เพื่อศึกษาจุดอ่อนและช่องโหว่ของระบบโทรศัพท์ผ่านอินเทอร์เน็ตที่มีจุดอ่อนในการรักษาความปลอดภัย

2.2. เพื่อศึกษาวิธีการโจมตีและใช้ประโยชน์จากช่องโหว่ของระบบระบบโทรศัพท์ผ่านอินเทอร์เน็ต

2.3. เพื่อการพัฒนาระบบป้องกันการโจมตีระบบโทรศัพท์ผ่านอินเทอร์เน็ตได้

2.4. เพื่อการกำหนดรูปแบบนโยบายการความปลอดภัยของระบบโทรศัพท์ผ่านอินเทอร์เน็ตได้

3. ขอบเขตของการวิจัย

3.1. กำหนดสถานที่วิจัยภายในห้องปฏิบัติการหน่วยงานของผู้วิจัย

3.2. กำหนดขอบเขตระยะเวลาการศึกษาและวิจัย 6 เดือน

3.3. กำหนดขอบเขตทดสอบการคุกคามแบบการปฏิเสธการให้บริการโจมตีด้วยการส่งคำสั่ง SIP INVITE เพียงรูปแบบเดียว

3.4. กำหนดขอบเขตการทดสอบการคุกคามจากเครือข่ายอินเทอร์เน็ตท้องถิ่นในห้องปฏิบัติการเท่านั้น

4. แนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

4.1 การสื่อสารโทรศัพท์ผ่านอินเทอร์เน็ต

การสื่อสารโทรศัพท์ผ่านอินเทอร์เน็ต เป็นการปรับเปลี่ยนรูปแบบและวิธีการสื่อสารโทรศัพท์โดยอาศัยเครือข่ายอินเทอร์เน็ต เป็นตัวกลางในการสื่อสารข้อมูลเสียง ซึ่งจะต้องใช้อุปกรณ์หรือโปรแกรมที่มีการใช้มาตรฐานการสื่อสาร (Protocol) ที่สามารถทำงานเข้ากันได้ทำการส่งสัญญาณโทรศัพท์จากต้นทางไปยังปลายทาง การโทรศัพท์ผ่านอินเทอร์เน็ตมีลำดับชั้นของการสื่อสารเหมือนกับการสื่อสารข้อมูลผ่านอินเทอร์เน็ต ที่เป็น ISO Model ในการสื่อสารข้อมูลจะต้องมีการกำหนดรูปแบบข้อมูล ข้อกำหนดต่างๆที่ให้ผู้สื่อสารและผู้รับสารได้เข้าใจและแปลความหมายให้ตรงกัน ในส่วนการสื่อสารโทรศัพท์ผ่านอินเทอร์เน็ตได้กำหนดมาตรฐานการสื่อสารในหัวข้อวิจัยจะกล่าวถึงมาตรฐานที่นิยมใช้กันทั่วไปดังนี้

4.1.1 มาตรฐานแบบ H.323(H.323) เป็นมาตรฐานที่สหภาพโทรคมนาคมระหว่างประเทศ (ITU) เป็นผู้กำหนดคุณสมบัติทางเทคนิคสำหรับการสื่อสารด้านเสียงบนเครือข่ายท้องถิ่น ซึ่งจะไม่มีข้อกำหนดในด้านคุณภาพของการให้บริการ(QoS) และเป็นจุดเริ่มต้นของการพัฒนาสำหรับการประชุมเสียง วีดีโอ บนเครือข่ายท้องถิ่น มาตรฐานแบบ H.323 ถูกพัฒนาต่อขยายเพื่อครอบคลุมการสื่อสารโทรศัพท์ผ่านอินเทอร์เน็ตในภายหลัง

4.2.2 มาตรฐานแบบSession Initial Protocol(SIP) เป็นมาตรฐานที่คณะทำงานเฉพาะกิจด้านวิศวกรรมอินเทอร์เน็ต (IETF) เป็นผู้พัฒนาสำหรับการสื่อสารข้อมูลเสียง วีดีโอบนเครือข่ายอินเทอร์เน็ต กำหนดในข้อกำหนด RFC3161 ซึ่งจะมีลักษณะการทำงานเหมือนกับมาตรฐาน HTTP ในส่วนของการเชื่อมต่อจากเครื่องลูกข่ายไปเครื่องแม่ข่าย โดยการร้องขอการเชื่อมต่อและการตอบกลับอีกทั้งมาตรฐานแบบ SIP ข้อมูลส่วนหัว(Header),วิธีการเข้ารหัสข้อมูล(Encryption)และ

สถานะสื่อสารข้อมูล(Status)เหมือนกัน โดยจะมี Session Description Protocol(SDP) เป็นตัวกำหนดรายละเอียดในการเชื่อมต่อ(Session) และใช้ Realtime Transfer Protocol(RTP) ในการควบคุมรับส่งข้อมูลเสียง วีดีโอบนเครือข่ายอินเทอร์เน็ต

4.2 ปัญหาของการสื่อสารโทรศัพท์ผ่านอินเทอร์เน็ต

4.2.1 **คุณภาพของการบริการ**(Quality of Service) เครือข่ายอินเทอร์เน็ต ถูกพัฒนาเพื่อการสื่อสารข้อมูลซึ่งไม่มีการรับประกันเรื่องเวลาการให้บริการ แต่จะเป็นการทำงานโดยใช้ความเหมาะสมหรือความเป็นไปได้สูงสุดของบริการ แต่การให้การสื่อสารโทรศัพท์เป็นการสื่อสารที่มีการตอบสนองแบบทันที (Realtime) ดังนั้นเพื่อให้มีการยอมรับของผู้ใช้งานระยะเวลาการส่งข้อมูลเสียงจะต้องไม่ต่ำค่าสุดที่กำหนดไว้ และต้องเป็นไปข้อกำหนดของ มาตรฐานที่คณะทำงานเฉพาะกิจด้านวิศวกรรมอินเทอร์เน็ต (IETF) รวมถึงการจัดลำดับความสำคัญของการส่งข้อมูล(Packet Prioritization) ก็มีผลต่อคุณภาพของการให้บริการเช่นกัน

4.2.2 **การทำงานร่วมกันของมาตรฐานการสื่อสาร**(Interoperability) ในการเชื่อมต่อระบบโทรศัพท์ผ่านอินเทอร์เน็ตผ่านโครงข่ายที่แตกต่าง และมีผลิตภัณฑ์ต่างยี่ห้อเพื่อที่จะทำให้อุปกรณ์สามารถเชื่อมต่อกันได้ จึงมีความจำเป็นที่จะต้องกำหนดให้เจ้าของผลิตภัณฑ์ทำการพัฒนาไปในแนวทางที่ IETF กำหนด ซึ่งปัญหาดังกล่าวนี้จะพบได้มากในช่วงเริ่มต้นของการระบบโทรศัพท์ผ่านอินเทอร์เน็ต

4.2.3 **ความปลอดภัยของบริการ**(Security) ปัญหาหลักจากสื่อสารข้อมูลบนโครงข่ายอินเทอร์เน็ต ซึ่งสามารถดักจับข้อมูลได้ง่าย ดังนั้นการเพิ่มความปลอดภัย,การเข้ารหัสข้อมูลของ,การป้องกันการโจมตี ระบบโทรศัพท์ผ่านอินเทอร์เน็ต ก็จะทำให้บริการมีความเชื่อถือมากขึ้น

4.2.4 **การเชื่อมต่อกับระบบโทรศัพท์สาธารณะ**(PSTN Integration) ในการใช้งานระบบโทรศัพท์ผ่านอินเทอร์เน็ตยังเป็นการใช้บริการเฉพาะส่วนดังนั้นการเชื่อมต่อกับระบบโทรศัพท์สาธารณะจำเป็นต้องมีอุปกรณ์แปลงสัญญาณการสื่อสารโทรศัพท์ให้เป็นแบบแพคเกจสวิตช์ เหมือนกับมาตรฐาน H.323

4.2.5 **การขยายระบบ(Scalability)** ในการให้บริการระบบโทรศัพท์ผ่านอินเทอร์เน็ต มีค่าใช้จ่ายที่ต่ำ ถ้าสามารถควบคุมคุณภาพของการให้บริการได้เทียบเท่ากับการสื่อสารโทรศัพท์แบบแพคเกจ การขยายโครงข่ายโทรศัพท์ผ่านอินเทอร์เน็ตสำหรับส่วนตัวและสาธารณะก็จะได้รับความนิยมมากยิ่งขึ้น ดังเช่นปัจจุบันในประเทศไทยมีบริการอินเทอร์เน็ตความเร็วสูงครอบคลุมพื้นที่สำคัญทางธุรกิจ การสื่อสารในรูปแบบอื่นๆที่อาศัยอินเทอร์เน็ต รวมถึงระบบโทรศัพท์อินเทอร์เน็ตก็จะถูกใช้บริการมากขึ้น

4.3 ภัยคุกคามของระบบโทรศัพท์ผ่านอินเทอร์เน็ต

4.3.1 การคุกคามแบบ Denial of Service (DoS) เป็นภัยคุกคามที่โจมตีต่อระบบโดยใช้อุปกรณ์โจมตีเครื่องเดียว หรือหลายๆเครื่องพร้อมกันโดยส่งคำสั่งไปที่เครื่องคอมพิวเตอร์แม่ข่าย เพื่อให้มีการรับคำสั่งจำนวนมากพร้อมกันทำให้มีการใช้ทรัพยากรเกินข้อจำกัด มีผลทำให้ระบบทำงานช้าลง คุณภาพเสียงไม่ดี ไม่ตอบสนองต่อผู้ใช้งานและไม่สามารถให้บริการได้ในที่สุด ตัวอย่างเช่น การโทรเข้าระบบพร้อมกันเกินจำนวนคู่สายทำให้ผู้ใช้งานจริงโทรไม่ได้ หรือการส่งคำสั่ง OPTIONS,REGISTER มาจำนวนมากทำให้ระบบต้องทรัพยากรจำนวนมากต่อการตอบสนองต่อคำสั่งที่เข้ามาจำนวนมากมีผลทำให้เกิดสภาวะความแออัดของการเชื่อมต่อ มีผลให้ระบบทำงานผิดปกติและไม่สามารถให้บริการได้ในที่สุด

4.3.2 การคุมคามแบบ War dialing) เป็นภัยคุกคามที่เข้าควบคุมระบบโทรศัพท์โดยทำการค้นหากำหนดหรือสุ่ม โทรไปยังหมายเลขโทรศัพท์ที่กำหนดโดยอัตโนมัติ ค้นหาและตรวจสอบสัญญาณที่เป็นโมเด็ม คอมพิวเตอร์โทรสาร ซึ่งผู้คุกคามอาจจะนำผลที่ได้ไปสร้างภัยคุมคามอย่างอื่นได้ อีกทั้งเป็นการรบกวนและสร้างความรำคาญผู้ใช้บริการในการรับโทรศัพท์จากปลายทางที่ไม่ใช่ผู้ติดต่อจริงและยังผลให้คู่สายถูกใช้งานโดยไม่เกิดประโยชน์ใดๆ

4.3.3 การคุกคามแบบ(Toll fraud) เป็นภัยคุกคามที่มีลักษณะเหมือน War dialing แต่จะเป็นการอาศัยระบบโทรศัพท์ ในการโทรออกไปยังเลขหมายภายนอก หรือโทรไปยังต่างประเทศที่มีการเรียกเก็บเงินปลายทางที่มีอัตราค่าบริการต่อนาทีสูง ซึ่งภัยคุกคามแบบจะทำให้เกิดความเสียหายต่อองค์กรณ์ที่ทำให้ถูกเรียกเก็บค่าบริการโทรศัพท์จากผู้รับปลายทางโดยไม่ได้ใช้งานจริงหรือทำให้ผู้ใช้งานจริงโทรศัพท์ออกภายนอกไม่ได้กรณีถูกคุกคามแบบ Toll fraud จนเกินวงเงินค่าบริการ

4.3.4 การคุกคามแบบ Phishing เป็นภัยคุกคามที่มีการโทรศัพท์ติดต่อเหยื่อโดยแอบอ้างและแสดงเลขหมายโทรศัพท์จากต้นทางที่เหยื่อมีความไว้วางใจ เช่นการอ้างว่าโทรมาจากธนาคารที่เหยื่อมีบัญชี และทำการหลอกล่อให้เหยื่อบอกหมายเลข และรหัสเอทีเอ็มหรือรหัสผ่าน หรืออ้างว่าโทรมาจากสำนักงานตำรวจ โดยผู้คุกคามนำข้อมูลดังกล่าวไปใช้ประโยชน์ ต่างๆ การถอนหรือโอนเงิน ทำให้เหยื่อสูญเสียทรัพย์ได้

4.3.5 การคุกคามแบบ Call interception เป็นภัยคุกคามที่อาศัยระบบโทรผ่านอินเทอร์เน็ตที่มีการรักษาความปลอดภัยน้อย ไม่มีการเข้ารหัสเสียง ทำให้ผู้คุกคามสามารถดักฟังและบันทึกเสียงสนทนา แล้วนำข้อมูลที่ได้ไปใช้ประโยชน์อย่างอื่นได้ เช่นข้อมูลคู่แข่งทางการค้า ความลับทางราชการ หรืออีกกรณีที่ปลายทางเป็นระบบบริการธนาคารผ่านโทรศัพท์ ผู้คุกคามสามารถดักจับ

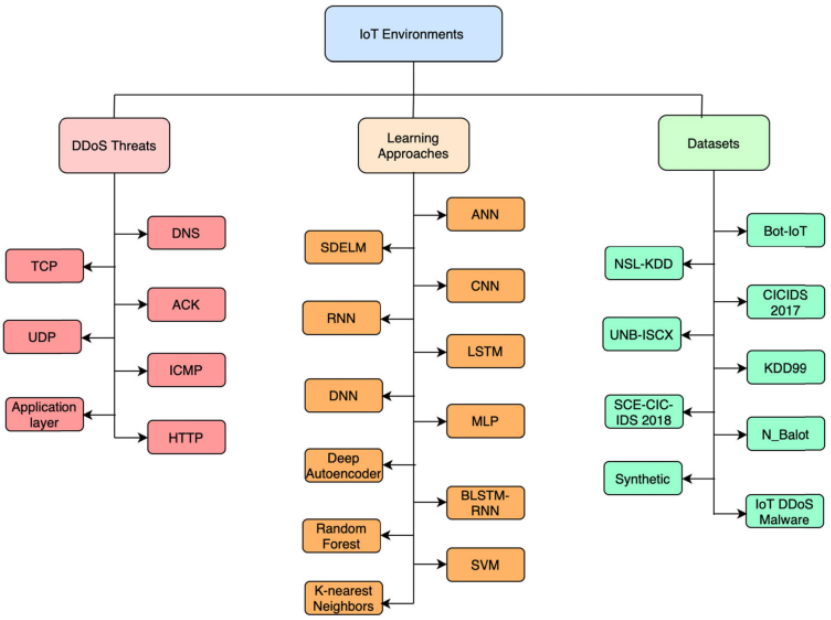
ข้อมูลหลายเลขบัญชี รหัสเอทีเอ็มได้ ทั้งนี้การดักฟังสามารถดักข้อมูลการโทรศัพท์แบบวีดีโอได้เช่นกัน

4.3.6 การคุกคามแบบ Theft of service เป็นภัยคุกคามที่มีลักษณะคล้ายกับ Toll fraud โดยผู้คุกคามอาศัยช่องโหว่ของเกิดจากการระบบโทรผ่านอินเทอร์เน็ต เข้าไปเปลี่ยนแปลงการตั้งค่าที่สำคัญ

4.3.7 การคุกคามแบบ Malware โดยผู้คุกคามจะใช้โปรแกรมที่มีจุดประสงค์ร้ายต่อคอมพิวเตอร์ในหลายรูปแบบเช่น ไวรัส(Virus), วอร์ม(Worm), สปายแวร์(Spyware), โทรจัน(Trojan) เพื่อให้ได้มาซึ่ง หมายเลขโทรศัพท์ บัญชีผู้ใช้ รหัสผ่าน เพื่อนำข้อมูลที่ได้ใช้ประโยชน์จากระบบโทรศัพท์ผ่านอินเทอร์เน็ตในรูปแบบอื่น

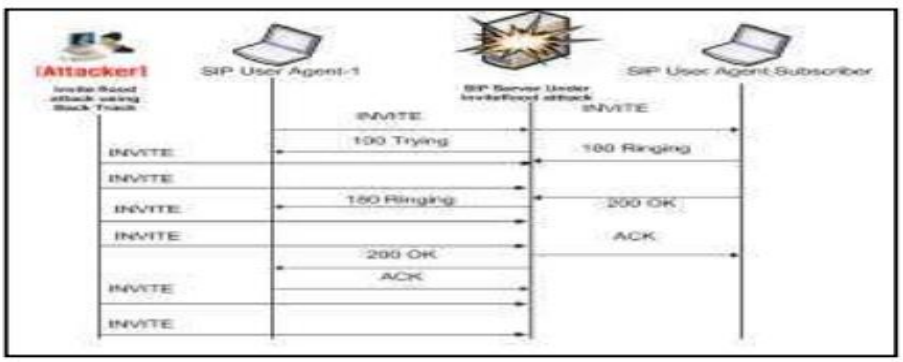
4.4 งานวิจัยที่เกี่ยวข้อง

4.4.1 Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments (Ahamed Aljuhani,2021) งานวิจัยนี้แสดงให้เห็นถึงการโจมตีแบบปฏิเสธการให้บริการ (DDoS) แบบกระจายมีจำนวนเพิ่มมากขึ้นโดยเฉพาะอย่างยิ่งการพัฒนาของเครือข่ายแบบฮาร์ดแวร์และซอฟต์แวร์เพื่อผ่านเครือข่าย(Cloud Computing, Internet of Things (IoT),Software Define Network (SDN) ทำให้เกินแนวโน้มที่จะส่งผลให้เกิดความสูญเสียทางเศรษฐกิจอย่างมหาศาลสำหรับธุรกิจและผู้ให้บริการ เทคนิคแมชชีนเลิร์นนิง (Machine learning: ML) มีการใช้กันอย่างแพร่หลายเพื่อป้องกันการโจมตี DDoS ในแบบต่างๆดังเช่น HTTP flood,SIPDDos,UDP flood,Low-rate DDos attacks โดยวิธีการ ML ในการเรียนรู้ดังนี้ K-means, SVM, Random forest tree, Convolutional neural network(CNN),RNN เป็นต้น ดังตัวอย่างภาพที่ 2 รูปแบบการเรียนรู้และชุดข้อมูลของ DDoS บนเครือข่าย IoT



ภาพที่ 2 ตัวอย่างภาพจากงานวิจัย สรุปรูปแบบการเรียนรู้และชุดข้อมูลของ DDoS บนเครือข่าย IoT

4.4.2 Study on Auto Detecting Defence Mechanisms against Application Layer DDoS Attacks in SIP SERVER (Muhammad Morshed Alam,Muhammad Yeasir Arafat,Feroz Ahmed, 2015) งานวิจัยนี้แสดงให้เห็นถึงการโจมตีแบบปฏิเสธการให้บริการ (DoS) ผ่าน Voice Over IP Protocol (VOIP) โดยจำลองการส่งคำสั่ง SIP INVITE จากโปรแกรมทดสอบโดยคำสั่งที่ส่งไปมีจำนวนเกินความสามารถของ IPPBX ทำให้เครื่องที่เป็นเป้าหมาย หยุดทำงานและมีผลต่อคุณภาพของการให้บริการ รวมถึงงานวิจัยนี้แสดงให้เห็นจำนวนการใช้งาน CPU และหน่วยความจำสูงขึ้นในช่วงการทดสอบโจมตี



ภาพที่ 2 ตัวอย่างภาพจากงานวิจัย รูปแบบคำสั่งการโจมตี DoS บน IPPBX ด้วยคำสั่ง INVITE

4.4.3 Detecting Flood-based Attacks against SIP Proxy Servers and Clients using Engineered Feature Sets (Hassan Asgharian,Ahmad Akbari,Bijan Raahemi, 2016) งานวิจัยนี้แสดงให้เห็นถึงการโจมตีแบบปฏิเสธการให้บริการ (DoS) และการโจมตีแบบปฏิเสธการให้บริการแบบกระจาย (DDoS) ผู้วิจัยแสดงข้อมูลให้เห็นระหว่างการโจมตีด้วยคำสั่ง INVITE และ REGISTER ซึ่งคำสั่ง INVITE จะทำให้มีผลกระทบต่อบริการมากกว่าจากข้อมูล IPPBX มีการตอบสนองต่อคำสั่ง INVITE ทันทีและมีคำสั่งต่อเนื่องจาก INVITE จำนวนมากกว่าทำให้การใช้ทรัพยากรบน IPPBX มีมากขึ้นโดยมีข้อมูลอ้างอิงในแต่ละแบบดังนี้

Title	# of Features	Engineered Features
Basic Flooding	3	$\left(\frac{SIP\ Messages}{Time\ Window}\right)$, $\left(\frac{Number\ of\ SIP\ Requests}{Total\ Number\ of\ SIP\ Messages}\right)$, $(INVITE-ACK)$
Advanced Flooding	5	$\left(\frac{SIP\ Messages}{Time\ Window}\right)$, $\left(\frac{Number\ of\ SIP\ Requests}{Total\ Number\ of\ SIP\ Messa}\right.$ $\left(\frac{Number\ of\ Transactions}{Number\ of\ SIP\ Messages\ in\ Window}\right)$, $\left(\frac{Number\ of\ 1xx}{Number\ of\ Messages\ in\ Current\ Window}\right)$, $\left(\frac{Number\ of\ 2xx}{Number\ of\ Messages\ in\ Current\ Window}\right)$,
Authentication Based Flooding	5	$\left(\frac{Number\ of\ 4xx}{Number\ of\ Messages}\right)$, $\left(\frac{Number\ of\ 5xx}{Number\ of\ Messages}\right)$, $\left(\frac{Number\ of\ REGISTER\ Messages}{Number\ of\ 2xx\ Messages}\right)$, $\left(\frac{Number\ of\ Senders}{Number\ of\ Transactions}\right)$, $\left(\frac{Number\ of\ Request\ Messages}{Number\ of\ Response\ Messages}\right)$
Memory Based Flooding	5	$\left(\frac{Number\ of\ 1xx}{Number\ of\ Messages\ in\ Current\ Window}\right)$, $\left(\frac{SIP\ Messages}{Time\ Window}\right)$, $\left(\frac{Number\ of\ 4xx}{Number\ of\ Messages}\right)$, $\left(\frac{Number\ of\ Senders}{Number\ of\ Transactions}\right)$, $\left(\frac{Number\ of\ Transactions}{Number\ of\ SIP\ Messages\ in\ Window}\right)$
ALL	14	All above features

ภาพที่ 3 ตัวอย่างภาพจากงานวิจัย ตารางเปรียเทียบการทดสอบการโจมตีในแต่ละแบบ

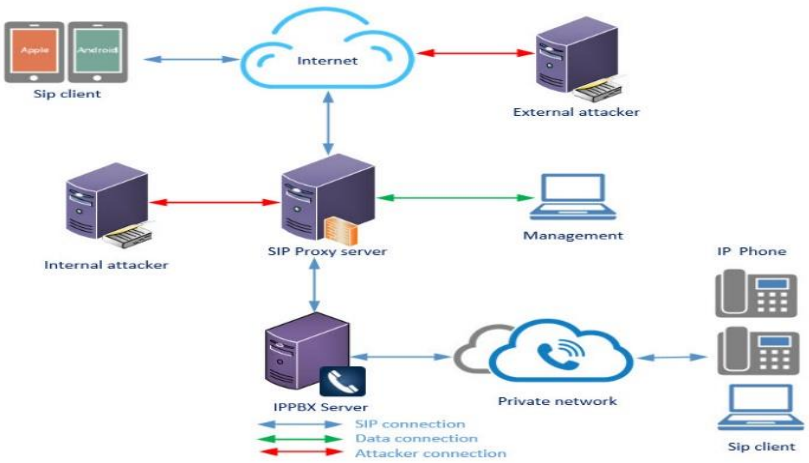
5. วิธีการดำเนินวิจัย

การโจมตีระบบโทรศัพท์ผ่านอินเทอร์เน็ตผู้บุกรุกสามารถเลือกใช้ได้หลายคำสั่ง เช่น INVITE,OPTION, CANCEL,BYE หรือคำสั่งอื่นที่เป็นมาตรฐานของ SIP อย่างไรก็ตามคำสั่ง INVITE จะมีความสะดวกมากกว่าเพราะส่วนประกอบของ SIP ตามมาตฐาน RFC 3261 จะรองรับคำส่ง INVITE ยิ่งกว่านั้นทุกระบบถูกออกแบบให้รับคำสั่ง INVITE โดยไม่ต้องส่งคำสั่งล่วงหน้า ดังนั้นคำสั่ง INVITE สามารถทำให้การใช้ทรัพยากรณ์ระบบให้หมดลงได้ง่าย รวมถึงระบบจะต้องมีการตอบกลับสถานะของคำสั่ง INIVTE ไปยังต้นทางเสมอ ด้วยค่า 1XX หรือ 2XX ซึ่งทำให้คำสั่ง SIP ทั้งหมดมีจำนวนเพิ่มมากขึ้นในช่วงเวลาของการโจมตี

5.1 รูปแบบการวิจัย

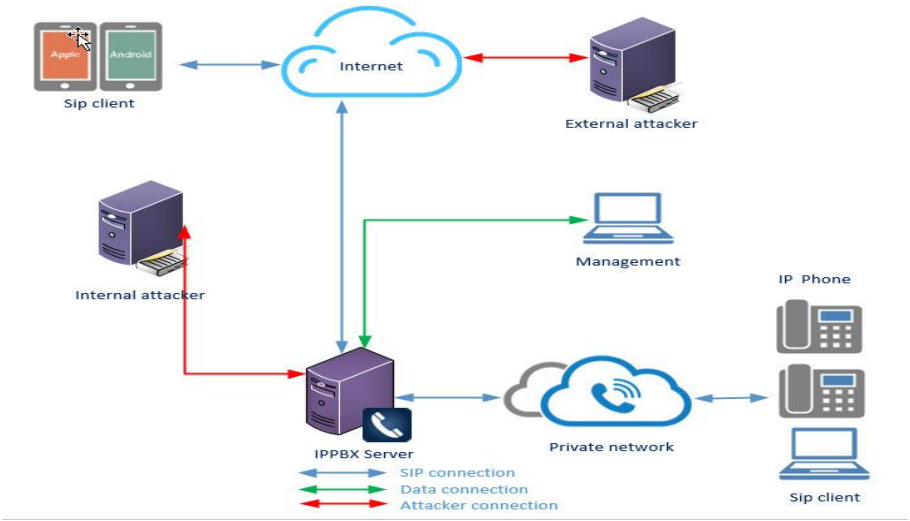
กำหนดโครงสร้างและองค์ประกอบของระบบทั้งหมดเพื่อสนับสนุนการวิจัยดังนี้

5.1.1 การเชื่อมต่อระบบและทดสอบผ่าน SIP PROXY เป็นการกำหนดให้ทำการทดสอบโดยส่งคำสั่งโจมตีผ่าน SIP PROXY ไปยัง IPPBX ดังภาพที่ 2



ภาพที่ 4 โครงสร้างและองค์ประกอบการทดสอบผ่าน SIP PROXY

5.2.2 การเชื่อมต่อระบบและทดสอบผ่าน IPPBX ปืนการกำหนดให้ทำการทดสอบโดยส่งคำสั่งโจมตีไปที่ ยัง IPPBX ดังภาพที่ 3



ภาพที่ 5 โครงสร้างและองค์ประกอบแบบไม่มีระบบเชื่อมต่อสัญญาณโทรศัพท์ผ่านอินเทอร์เน็ต(SIP PROXY)

5.2 กลุ่มข้อมูลที่ใช้ในการวิจัย

จากหัวข้อ 4.3.3 จะเห็นได้ว่า คำสั่ง INVITE จะทำให้มีผลกระทบต่อบริการมากกว่า [1] IPPBX มีการตอบสนองต่อคำสั่ง INVITE ทันทีและมีคำสั่งต่อเนื่องจาก INVITE จำนวนมากกว่าทำให้การใช้ทรัพยากรบน ดังนั้นผู้วิจัยได้ทำการเลือกคำสั่ง INVITE ในการทดสอบงานวิจัยครั้งนี

5.3 เครื่องมือและอุปกรณ์ที่ในการวิจัย

5.3.1 อุปกรณ์ (Hardware) ที่เป็นอุปกรณ์หลักมีดังนี้

5.3.1.1. เครื่องคอมพิวเตอร์เสมือน (VIRTUAL SERVER :VM) สำหรับติดตั้งระบบ SIP PROXY ของ IPPBX

5.3.1.2. เครื่องคอมพิวเตอร์VM สำหรับติดตั้งระบบ IPPBX

5.3.1.3. อุปกรณ์โทรศัพท์ผ่านอินเทอร์เน็ต(IP phone) เป็นอุปกรณ์ที่รองรับการเชื่อมสัญญาณโทรศัพท์

5.3.1.4. เครื่องคอมพิวเตอร์สำหรับติดตั้งโปรแกรมสื่อสารโทรศัพท์ผ่านอินเทอร์เน็ต (Softphone)

5.3.1.5. เครื่องคอมพิวเตอร์VM สำหรับติดตั้งโปรแกรมทดสอบการผู้โจมตีระบบโทรศัพท์ผ่านอินเทอร์เน็ต (SIPP)

5.3.2 ซอฟต์แวร์(Software) โดยจะมีส่วนประกอบย่อยดังนี้

5.3.2.1. ระบบปฏิบัติการ(Operating system:OS) เป็นระบบหลักในการควบคุมและประมวลผล ในด้านต่างๆตามหน้าที่หลักของแต่ละส่วนในหัวข้อศึกษานี้โดยจะระบบปฏิบัติการเดเบียนลีนุกซ์ รุ่น 11.0(Debian GNU/Linux OS Release 11.0 :Debian) และระบบปฏิบัติการวินโดวน์ 10 (Windows 10 OS)

5.3.2.2. ระบบ SIP PROXY ที่ผู้วิจัยใช้โปรแกรม Kamailio® ทำหน้าที่รักษาความรักษาความปลอดภัย และทำหน้าที่แบบตัวกลาง(SIP Proxy) ในการเชื่อมต่อสัญญาณโทรศัพท์ระหว่างแม่ข่ายกับเครื่องลูกข่าย (SIP Client) จากเครือข่ายอินเทอร์เน็ต

5.3.2.3. ระบบ IPPBX ทำหน้าที่เป็นเครื่องแม่ข่ายบริหารจัดการเชื่อมต่อสัญญาณโทรศัพท์ผ่านอินเทอร์เน็ตระหว่างแม่ข่ายกับ SIP Client รองรับมาตรฐานการเชื่อมต่อแบบ SIP

5.3.2.4. โปรแกรม Softphone เป็นโปรแกรมสำหรับสื่อสารข้อมูลเสียงและวีดีโอโครงข่ายอินเทอร์เน็ตโดยรองรับการเชื่อมต่อกับระบบ IPPBX รองรับมาตรฐานการเชื่อมต่อแบบ SIP

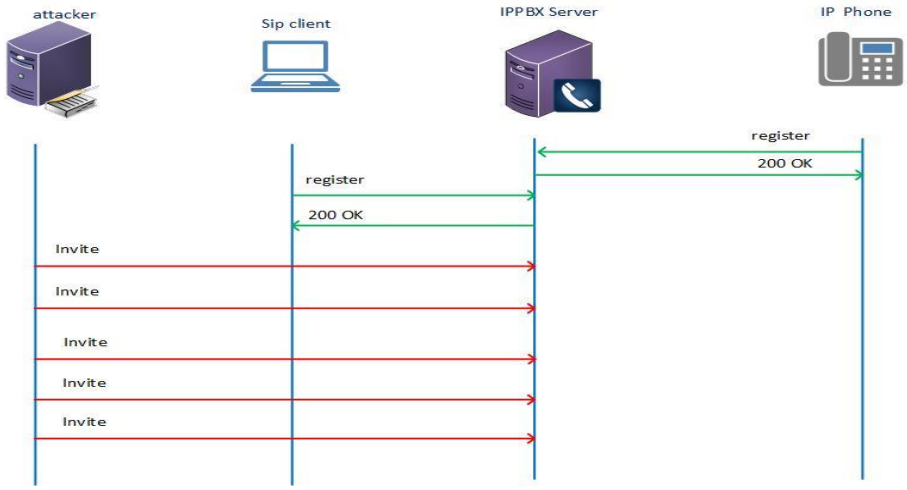
5.3.2.5. โปรแกรม SIPP เป็นโปรแกรมสำหรับสื่อสารข้อมูลเสียงและวีดีโอโครงข่ายอินเทอร์เน็ตที่รองรับการสร้างจำนวนครั้งในการเชื่อมต่อไปยัง SIP PROXY และ ระบบโทรศัพท์ผ่าน IPPBX แบบจำนวนมากได้ รวมทั้งสามารถกำหนดค่าพารามิเตอร์และคุณสมบัติของการเชื่อมต่อได้

5.3.2.6. โปรแกรมดักจับข้อมูลและแสดงผลการสื่อสารข้อมูลผ่านโครงข่ายอินเทอร์เน็ตที่รองรับการดักจับข้อมูลประเภท SIP และ RTP ได้ เช่นโปรแกรมไวร์ชาร์ก (Wireshark) หรือคำสั่ง tcpdump เป็นต้น

6. ผลการทดลอง

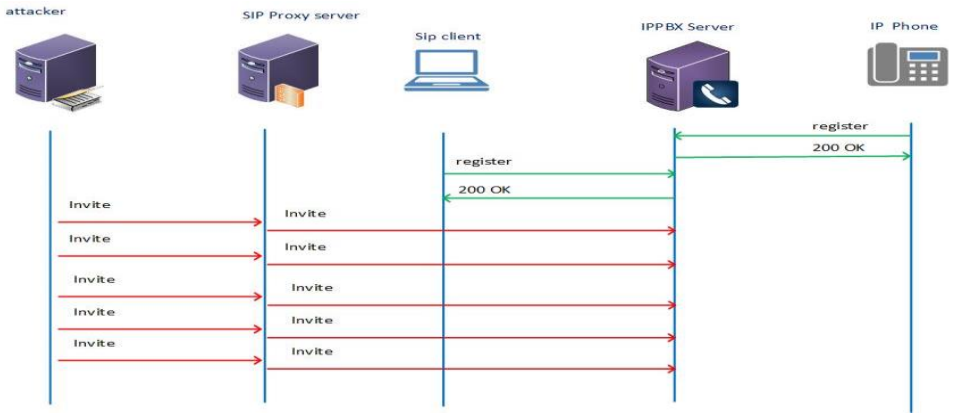
การทดลองทำการเปรียบเทียบระหว่างการโจมตีระบบโทรศัพท์ผ่านอินเทอร์เน็ต ในแต่ละเงื่อนไขเพื่อให้เห็นข้อมูลการทำงานของระบบและสรุปข้อมูลการทดสอบ โดยแบ่งการทดสอบเป็น 3 ส่วนดังนี้

6.1 **การทดสอบโจมตี IPPBX จากโปรแกรมทดสอบการโจมตี SIPP** การดำเนินการทดสอบส่วนนี้จะเป็นการส่งคำสั่ง SIP INVITE จากโปรแกรมทดสอบการโจมตี SIPP ไปยัง IPPBX จากเครือข่ายอินเทอร์เน็ตท้องถิ่น โดยกำหนดค่าอัตราการในการโทรศัพท์ต่อวินาที (CALL RATE) และระยะเวลาในการโจมตี เป็นเงื่อนไขในการทดสอบ อีกทั้งยังทำการส่งคำสั่ง SIP REGISTER เพื่อลงทะเบียนบัญชีผู้ใช้งาน เพื่อให้เห็นข้อมูลการใช้ทรัพยากรของ IPPBX ที่ตอบสนองต่อการโจมตีจากโปรแกรม SIPP โดยมีแผนผังการเชื่อมต่อทดสอบการโจมตีดังภาพที่ 6



ภาพที่ 6 แสดงแผนผังการเชื่อมต่อทดสอบการโจมตี IPPBX จากโปรแกรม SIPP

6.2 การทดสอบโจมตี IPPBX จากโปรแกรมทดสอบการผู้โจมตี SIPP ผ่าน SIP PROXY การดำเนินการทดสอบจะเป็นการส่งคำสั่ง SIP INVITE จากโปรแกรมทดสอบการโจมตี SIPP ผ่าน SIP PROXY ไปยัง IPPBX จากเครือข่ายอินเทอร์เน็ตท้องถิ่น โดยมีการแผนผังการเชื่อมต่อดังภาพที่ 7 นี้



ภาพที่ 7 แสดงแผนผังการเชื่อมต่อทดสอบการโจมตี IPPBX ผ่าน SIP PROXY

โดยกำหนดค่า CALL RATE และระยะเวลาในการโจมตี และเป็นเงื่อนไขในการทดสอบ มีการกำหนดค่าบนโมดูล PIKE ซึ่งการตั้งค่าข้างต้นจะมีผลต่ออัตราการโทรศัพท์ต่อวินาทีที่ SIP PROXY ใช้ควบคุมคำสั่ง SIP INVITE จากโปรแกรมทดสอบโจมตี SIPP ด้วย

6.3 ผลทดลองเปรียบเทียบประสิทธิภาพ

จากตารางที่ 1 ผลการทดสอบโจมตีจากการกำหนดรูปแบบการทดสอบเป็น 3 แบบ เพื่อจะสามารถเปรียบเทียบผลลัพท์จากการทดสอบได้ดังนี้

แบบที่ 1 การทดสอบโจมตี IPPBX กำหนดจำนวนครั้งที่โทรศัพท์ทดสอบต่อวินาที เป็น 100, 500, 1,000, 5,000 และ10,000 ครั้งต่อวินาที มีผลให้ IPPBX มีผลให้การใช้งานโทรศัพท์ผ่านอินเทอร์เน็ต(Softphone) และอุปกรณ์โทรศัพท์ รวมถึงการลงทะเบียนบัญชีหมายเลขโทรศัพท์ (SIP Register) ไม่สามารถทำงานได้และล้มเหลวซึ่งจำนวนคำสั่ง SIP INVITE ที่ถูกส่งไปยัง IPPBX จะเกินความสามารถในการรองรับคำสั่งไม่เกิน 30 คำสั่งต่อวินาที

แบบที่ 2 การทดสอบโจมตีโดยผ่าน SIP PROXY กำหนดค่าพารามิเตอร์บนโมดูล Pike Sampling time unit 2 วินาที ,Reqs_density_per_unit 100 ครั้ง, Remove_latency 120 วินาที กำหนดจำนวนครั้งที่โทรศัพท์ทดสอบต่อวินาที เป็น 10,20 และ 30 ครั้งต่อวินาที มีผลให้ IPPBX มีผลให้การใช้งานโทรศัพท์ผ่านอินเทอร์เน็ต(Softphone) และอุปกรณ์โทรศัพท์ รวมถึงการลงทะเบียนบัญชีหมายเลขโทรศัพท์ (SIP Register) สามารถทำงานได้ตามปกติ ทั้งนี้ในการทดสอบส่งคำสั่ง 30 ครั้งต่อวินาที SIP PROXY จะหยุดส่งคำสั่งไปยัง IPPBX ตามเงื่อนไขที่กำหนดบน SIP PROXY เพื่อเป็นการจำกัดการส่งคำสั่ง SIP INVITE และมีผลให้ IPPBX ยังคงทำงานได้ตามปกติ

แบบที่ 3 การทดสอบโจมตีโดยผ่าน SIP PROXY กำหนดค่าพารามิเตอร์บนโมดูล Pike Sampling time unit 2 วินาที,Reqs_density_per_unit 200 ครั้ง,Remove_latency 120 วินาที เพื่อสามารถรับคำสั่ง SIP INVITE และส่งไปยัง IPPBX เกินกว่าความสามารถในการรองรับคำสั่ง จะเห็นได้ว่า จำนวนครั้งที่โทรศัพท์ทดสอบต่อวินาที เป็น 20 และ 30 ครั้งต่อวินาที การใช้งานโทรศัพท์ผ่านอินเทอร์เน็ต(Softphone) และ อุปกรณ์โทรศัพท์ รวมถึงการลงทะเบียนบัญชีหมายเลขโทรศัพท์ (SIP Register) บน IPPBX สามารถทำงานได้ตามปกติ แต่ในการคำสั่ง SIP INVITE 50 ครั้งต่อวินาที จะทำให้ผลการทำงานคำสั่งภายในที่ทดสอบ IPPBX ไม่สามารถทำงานได้และล้มเหลว ซึ่งเป็นผลจาก SIP PROXY ส่งคำสั่ง SIP INVITE ไปยัง IPPBX เกินความสามารถในการรองรับคำสั่งได้

รูปแบบการทดสอบ	จำนวนครั้งที่โทรศัพท์ทดสอบต่อวินาที	สถานะระบบ SIP PROXY SERVER	สภานะระบบ IPPBX SERVER	การใช้งานโทรศัพท์ผ่านอินเตอร์เน็ต (Softphone) และอุปกรณ์โทรศัพท์	การลงทะเบียนบัญชีหมายเลขโทรศัพท์(SIP Register)
การทดสอบโจมตีโดยไม่ผ่าน SIP PROXY SERVER	0	ปกติ	ปกติ	โทรศัพท์ระหว่างเครื่องภายในได้	สำเร็จ
	100	ปกติ	ไม่ตอบสนองต่อคำสั่งเชื่อมต่อ (Invite)	ไม่สามารถโทรศัพท์ระหว่างเครื่องภายในได้	ล้มเหลว
	500	ปกติ	ไม่ตอบสนองต่อคำสั่งเชื่อมต่อ (Invite)	ไม่สามารถโทรศัพท์ระหว่างเครื่องภายในได้	ล้มเหลว
	1,000	ปกติ	ไม่ตอบสนองต่อคำสั่งเชื่อมต่อ (Invite)	ไม่สามารถโทรศัพท์ระหว่างเครื่องภายในได้	ล้มเหลว
	5,000	ปกติ	ไม่ตอบสนองต่อคำสั่งเชื่อมต่อ (Invite)	ไม่สามารถโทรศัพท์ระหว่างเครื่องภายในได้	ล้มเหลว
	10,000	ปกติ	ไม่ตอบสนองต่อคำสั่งเชื่อมต่อ (Invite)	ไม่สามารถโทรศัพท์ระหว่างเครื่องภายในได้	ล้มเหลว
การทดสอบโจมตีโดยผ่าน SIP PROXY SERVER กำหนดค่าโมดูล Pike Sampling time unit 2 วินาที Reqs_density_per_unit 100 ครั้ง Remove_latency 120 วินาที	10	ปกติ	ปกติ	โทรศัพท์ระหว่างเครื่องภายในได้	สำเร็จ
	20	ปกติ	ปกติ	โทรศัพท์ระหว่างเครื่องภายในได้	สำเร็จ
	30	ปฏิเสธการคำสั่งเชื่อมต่อ (Invite)	ปกติ	โทรศัพท์ระหว่างเครื่องภายในได้	สำเร็จ
การทดสอบโจมตีโดยผ่าน SIP PROXY SERVER กำหนดค่าโมดูล Pike Sampling time unit 2 วินาที Reqs_density_per_unit 200 ครั้ง Remove_latency 120 วินาที	20	ปกติ	ปกติ	โทรศัพท์ระหว่างเครื่องภายในได้	สำเร็จ
	30	ปกติ	ปกติ	โทรศัพท์ระหว่างเครื่องภายในได้	สำเร็จ
	50	ปฏิเสธการคำสั่งเชื่อมต่อ (Invite)	ไม่ตอบสนองต่อคำสั่งเชื่อมต่อ (Invite)	ไม่สามารถโทรศัพท์ระหว่างเครื่องภายในได้	ล้มเหลว
** หมายเหตุ ระบบ IPPBX SERVER สามารถรองรับการเชื่อมต่อได้ 30 คำสั่งต่อวินาที					

ตารางที่ 1 แสดงข้อมูลเปรียบเทียบผลการทดสอบในแต่ละแบบ

จากข้อมูลข้างต้นจะเห็นได้ว่าการกำหนดค่าพารามิเตอร์ของโมดูล Pike บน SIP PROXY จะมีผลต่อการตอบสนองต่อการส่งคำสั่งจาก SIP PROXY ไปยัง IPPBX การกำหนดค่าให้อยู่ในช่วงค่าความสามารถในการรองรับคำสั่งต่อวินาทีของ IPPBX ก็จะมีผลทำให้ SIP PROXY หยุดส่งคำสั่งไปยัง IPPBX ตามเงื่อนไขที่กำหนดได้ หากกำหนดไว้มากกว่าก็จะมีผลทำให้ IPPBX

ทำงานล้มเหลวต่อการทำงานคำสั่งภายใน ทั้งนี้การทดสอบโจมตีไปยัง IPPBX โดยตรงทำให้ระบบทำงานล้มเหลว กรณีคำสั่ง SIP INVITE มีจำนวนเกินความสามารถในการรองรับคำสั่งต่อวินาทีของ IPPBX ดังนั้นการป้องกันการโจมตี IPPBX จากคำสั่ง SIP INVITE ด้วยวิธีแบบ Denial of Service (DoS) ด้วยโมดูล Pike บน SIP PROXY นั้นจะต้องปรับค่าอัตราการรับคำสั่งต่อวินาที ให้เหมาะสมกับค่าความสามารถในการรองรับคำสั่งต่อวินาทีของ ของ IPPBX

7. สรุปผลการวิจัยและข้อเสนอแนะ

7.1 สรุปผลการวิจัย

งานวิจัยนี้สรุปได้ว่าการส่งคำสั่ง SIP INVITE จะมีผลต่อการใช้ทรัพยากรของ IPPBX เพิ่มขึ้นอย่างเป็นสัดส่วนต่ออัตราคำสั่งต่อวินาทีที่ถูกส่งจากโปรแกรมจำลองการโจมตี จะเห็นได้ว่ามีผลทำให้ IPPBX มีการทำงานล้มเหลวไม่ตอบสนองต่อคำสั่งการทำงานภายในของ IPPBX และไม่สามารถให้บริการได้ โดยการเปรียบเทียบกับการทดสอบโจมตี IPPBX ผ่าน SIP PROXY ที่กำหนดค่าความสามารถในการรองรับคำสั่งต่อวินาทีบน IPPBX และ SIP PROXY มีค่าเท่ากัน มีผลทำให้ SIP PROXY ปฏิเสธการให้บริการด้วยการหยุดส่งคำสั่ง SIP INVITE ไปยัง IPPBX กรณีอัตราคำสั่งต่อวินาทีเกินที่กำหนด ทำให้ IPPBX สามารถทำงานตอบสนองต่อคำสั่งภายในระบบโดยไม่มีผลกระทบต่อบริการ ทั้งนี้ในการทดสอบโดยใช้คำสั่งการโจมตีด้วยคำสั่งอื่นเช่น OPTION,NOTIFY,CANCEL จะมีผลต่อการใช้ทรัพยากรของ IPPBX ในปริมาณที่แตกต่างกันตามรูปแบบของการตอบสนองต่อคำสั่งของ IPPBX จากข้อสรุปการวิจัยนี้พบว่าผลกระทบการโจมตี IPPBX จากการปฏิเสธการให้บริการด้วยการยิงข้อความ SIP INVITE จะทำให้ IPPBX ทำงานล้มเหลว และ SIP PROXY สามารถป้องกันการโจมตีจากการปฏิเสธการให้บริการได้

7.2 ข้อเสนอแนะ

เพื่อให้การศึกษาวิจัยครั้งนี้ครอบคลุมความปลอดภัยมากขึ้น แนะนำศึกษาเพิ่มเติมดังนี้

7.2.1 การป้องกันโจมตีโดยใช้รหัสผู้ใช้งานและรหัสผ่านแบบคาดเดาไม่คำนึงถึงรูปแบบ(Brute force user name / password) ,การโจมตีด้วยเบอร์โทรศัพท์ที่คาดเดาไม่คำนึงถึงรูปแบบ (Brute force numbering /prefix)

7.2.2 การตรวจสอบหมายเลขประจำเครื่องคอมพิวเตอร์(IP Address) ที่เห็นว่าเป็นเครื่องที่โจมตีจากผู้ไม่หวังดีแล้วทำการปิดการเชื่อมต่อโดยถาวร(IP Banned / Blocking)

7.2.3 การเพิ่มการแจ้งเตือนแบบต่อผู้ดูแลระบบเพื่อเป็นการรับมือต่อการโจมตีได้อย่างมีประสิทธิภาพและแก้ไขปัญหาหรือผลกระทบที่เกิดขึ้นได้ทันท่วงที

7.2.4 การปกปิดโครงสร้างของระบบเครือข่าย (Network topology hiding)

7.2.5 การควบคุมและจำกัดการลงทะเบียน(Registration rate throttling)

7.2.6 กำหนดสถาพแวดล้อมการทดสอบบนเครือข่ายสาธารณะ

7.2.7 กำหนดให้ระบบ IPPBX ,SIP PROXY ,SIPP ที่ทดสอบติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายแยกเฉพาะเครื่อง

บรรณานุกรม

Aljuhani , A. (2021) Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments.

Asgharian, H., Akbari, A., and Raahem, B. (2016) Detecting Flood-based Attacks against SIP Proxy Servers and Clients using Engineered Feature Sets.

Alam, M., Arafat, Muhammad Y., and Ahmed, F. (2015). Study on Auto Detecting Defense Mechanisms against Application Layer DDoS Attacks in SIP SERVER.