ปัญหาของวีโอไอพี และสแปมบนระบบโทรศัพท์บนอินเตอร์เน็ต

Problems of VOIP and Spam over Internet Telephony

วรพล ลีลาเกียรติสกุล

Faculty of Information Science and Technology
Mahanakorn University of Technology

บทคัดย่อ – เป็นเวลาหลายปีที่ผ่านมาที่ระบบวีโอไอพีมีการใช้งานอย่างแพร่หลาย เพราะราคาของการใช้บริการที่ถูกกว่าระบบการโทรศัพท์แบบดั้งเดิม แต่อย่างไรก็ตาม ประชาชนหรือผู้ใช้จำเป็นที่จะต้องระมัดระวังเกี่ยวกับเรื่องความมั่นคงปลอดภัยของการทำงานบนระบบของวีโอไอพี เพราะข้อมูลเสียงต้องเดินทางผ่านเครือข่ายสาธารณะและช่องโหว่ของระบบวีโอไอพีเอง ดังนั้นบทความนี้จึงเสนอวิธีการทำงานของระบบวีโอไอพี และโปรโตคอลที่สนับสนุนการทำงาน นอกจากนั้นก็มีการวิเคราะห์ความมั่นคงปลอดภัยเพื่อแสดงช่องโหว่และภัยคุกคามของระบบวีโอไอพี ท้ายที่สุดมีการอธิบายสแปมบนระบบโทรศัพท์อินเตอร์เน็ตและวิธีการต่อต้าน เนื่องจากว่า สแปมบนโทรศัพท์อินเตอร์เน็ตเป็นหนึ่งในปัญหาที่ได้รับการรับรู้มากที่สุดของระบบวีโอไอพีในปัจจุบัน

คำสำคัญ – วีโอไอพี, ซิพ, สปิต, สแปม, การต่อต้านสปิต

ABSTRACT – VoIP has been widely used for years, because of its lower service cost than the traditional telephone call. However, people or users need to be aware of security on VoIP system because the voice data has to traverse on public networks and vulnerabilities on VoIP system itself. Therefore, this article presents how VoIP system works including supported protocols. Additionally, security analysis is also provided to show vulnerabilities and threats on VoIP system. Finally, SPIT (SPam over Internet Telephony) and Anti-SPIT frameworks are explained since SPIT is currently one of the most recognized problems on VoIP system.

KEYWORDS – SIP, VoIP, SPIT, Anti-SPIT

---

1. บทนำ

ช่วงเวลาที่ผ่านมาไม่นานจนถึงปัจจุบันนี้ การสื่อสารข้อมูลเสียงบนระบบอินเตอร์เน็ตหรือ วีโอไอพี (VoIP) [1] ได้รับความนิยมมากทั้งในประเทศและต่างประเทศ ไม่ว่าจะเป็นการสื่อสารระหว่างเครื่องคอมพิวเตอร์ กับ เครื่องคอมพิวเตอร์ หรือ การสื่อสารระหว่างเครื่องคอมพิวเตอร์ กับโทรศัพท์ แม้กระทั่งการสื่อสารระหว่างโทรศัพท์ กับโทรศัพท์ด้วยกันเอง เนื่องจากว่าการใช้บริการสื่อสารข้อมูลเสียงหรือการโทร (Call) บนระบบอินเตอร์เน็ตมีค่าใช้จ่ายน้อยมากเมื่อเทียบกับระบบโทรศัพท์ปกติ กล่าวคือถ้าเป็นการสื่อสารจากคอมพิว

เตอร์กับคอมพิวเตอร์ จะไม่เสียค่าใช้จ่ายในการโทรติดต่อกัน อย่างไรก็ตามถ้ามีการโทรระหว่างผู้ใช้ที่เป็นเครื่องคอมพิวเตอร์ไปยังโทรศัพท์บ้านหรือโทรศัพท์มือถือจะมีค่าใช้จ่ายบ้าง แต่จะมีอัตราค่าบริการที่ถูกกว่าระบบโทรศัพท์ปกติ เช่นบริการของทีโอทีเน็ตคอล (ToT Netcall) [2] ทรูเน็ตทอร์ค (True Nettalk) [3] นอกจากนั้นก็มีบริการระหว่างโทรศัพท์กับโทรศัพท์ โดยผ่านเครือข่ายของอินเตอร์เน็ตที่มีราคาถูกกว่าแบบปกติ เช่น ระบบการโทรทางไกลต่างประเทศของการสื่อสารแห่ง ประเทศไทย (CAT009) [4] องค์การโทรศัพท์ (TOT007) [5] เป็นต้น

ราคาของการใช้บริการที่ถูกกว่าค่อนข้างมากสำหรับการใช้โทรศัพท์บนอินเตอร์เน็ต เมื่อเปรียบเทียบกับระบบโทรศัพท์ที่ใช้งานในปัจจุบัน มาจากการสื่อสารข้อมูลเสียงบนอินเตอร์เน็ต เป็นการทำงานอยู่บนระบบแพ็คเก็ตสวิทช์ (Packet Switching) ซึ่งเป็นระบบที่ผู้ใช้อื่นๆสามารถใช้ทรัพยากรของเครือข่ายร่วมกันได้ ทำให้มีการออกแบบระบบที่รองรับผู้ใช้ได้มากกว่าระบบเซอร์กิตสวิทช์ (Circuit Switching) ซึ่งเป็นการสื่อสารข้อมูลเสียงบนระบบโทรศัพท์ปกติ โดยที่ผู้ใช้แต่ละรายจะมีการจัดช่องสัญญาณของตัวเองไม่สามารถใช้ทรัพยากรของผู้อื่นได้ทำให้รองรับจำนวนผู้ใช้ได้น้อยกว่าระบบแพ็คเก็ตสวิทช์ ทำให้ต้นทุนของการให้บริการถูกลง แต่อย่างไรก็ตามปัญหาสำคัญของการให้บริการเสียงบนระบบแพ็คเก็ตสวิทช์คือการเกิดการหน่วงเวลาของการสื่อสารข้อมูล (Delay) หรือแม้กระทั่งการสูญหายของข้อมูล (Loss) เมื่อมีผู้ใช้มากเกินไปในช่วงเวลาหนึ่งๆ ซึ่งเป็นเรื่องที่สามารถเกิดขึ้นได้เสมอบนระบบแพ็คเก็ตสวิทช์ ดังนั้นผู้ใช้จะต้องรับรู้ปัญหาหรือข้อจำกัดที่อาจจะเกิดขึ้น ในขณะที่การสื่อสารแบบเซอร์กิตสวิทช์จะไม่เกิดการหน่วงเวลาของการสื่อสารข้อมูลเสียง และสามารถรับประกันคุณภาพของบริการได้ (Quality of Service) เนื่องจากว่าก่อนที่จะมีการสื่อสารข้อมูลเสียงจะมีสร้างคอนเน็คชั่น (Establishing Connection) และการจองช่องสัญญาณ (Chanel Reservation) เพื่อใช้ในการสื่อสารข้อมูลเสียงไว้ก่อนแล้ว ดังนั้นผู้ใช้งานการโทรบนระบบเซอร์กิตสวิทช์จะได้คุณภาพของเสียงและการทำงานที่ดีแน่นอน

ถึงแม้ว่าคุณภาพการให้บริการด้านเสียงบนเครือข่ายอินเตอร์เน็ตหรือวีโอไอพีจะเป็นปัญหา แต่ราคาของการใช้บริการที่ถูกกว่าค่อนข้างมากก็ทำให้ผู้ใช้ยอมรับข้อบกพร่องที่อาจจะเกิดขึ้นได้ และมีการใช้งานอย่างแพร่หลาย ซึ่งการทำงานของวีโอไอพีมีความน่าสนใจในด้านกระบวนการทำงานและด้านความมั่นคงปลอดภัย (Security) เนื่องจากว่าข้อมูลเสียงจะต้องเดินทางผ่านเครือข่ายอินเตอร์เน็ตซึ่งเป็นเครือข่ายสาธารณะ (Public Network) ดังนั้นในบทความนี้จึงได้ทำการอธิบายโครงสร้างการทำงานและปัญหาทางด้านความมั่นคงปลอดภัยที่สามารถเกิดบนระบบวีโอไอพี รวมไปถึง สแปมบนระบบโทรศัพท์บนอินเตอร์เน็ต หรือเรียกสั้นๆว่า *สปิต* (SPIT, SPam over Internet Telephony) ที่เป็นหนึ่งในปัญหาที่พบมากที่สุดในการใช้งานของวีโอไอพี

การจัดเรียงเนื้อหาของบทความ ได้แบ่งเป็นหัวข้อต่างๆ ดังต่อไปนี้ บทที่ 2 อธิบายพื้นฐานการทำงานของซิพ ซึ่งบรรยายถึงภาพรวมการทำงานและกระบวนการต่างๆของซิพ จากนั้นบทที่ 3 จะอธิบายถึงมุมมองด้านความปลอดภัยของซิพและโครงสร้างของวีโอไอพี โดยแสดงปัญหาด้านต่างๆของความมั่นคงปลอดภัย จากนั้นเน้นไปที่ภัยคุกคามเรื่อง *สปิต* หรือสแปมบนโทรศัพท์บนอินเตอร์เน็ต จะถูกกล่าวถึงในบทที่ 4 โดยบทที่ 5 จะอธิบายถึงแนวคิดกรอบการทำงานเพื่อป้องกันสปิตและเกณฑ์การประเมินประสิทธิภาพของวิธีการป้องกัน บทที่ 6 แสดงวิธีการป้องกันแบบต่างๆพร้อมกับจุดด้อยของวิธีการเหล่านั้น บทที่ 7 เป็นบทสรุปของบทความ

2. SIP (Session Initiation Protocol)

2.1 ภาพรวมของซิพ

ซิพ (SIP) [6] เป็นโปรโตคอลที่ออกแบบมาเพื่อรองรับการทำงานของการสื่อสารด้านสื่อประสม เช่นวีดีโอ และเสียง เป็นต้น เพื่อให้ผู้ใช้งานสามารถสร้างเซสชั่น (Session) เพื่อใช้ในการสนทนาหรือสื่อสารระหว่างกัน โดยซิพ จะทำสิ่งต่างๆ เหล่านี้

- จัดเตรียมกลไกสำหรับการติดตั้งการโทร(Call) ระหว่างผู้โทรต้นทาง (Caller) และผู้รับปลายทาง (Callee) บนเครือข่ายไอพี โดยกลไกนี้อนุญาตให้ผู้โทรต้นทางแจ้งไปยังผู้รับปลายทางว่าต้องการจะติดต่อด้วย นอกจากนั้นยังสามารถกำหนดข้อตกลงวิธีการเข้ารหัสข้อมูลเสียงที่จะใช้ระหว่างการโทร รวมถึงวิธีการที่ผู้ใช้งานจะยกเลิกการโทร
- จัดเตรียมกลไกสำหรับผู้โทรต้นทางในการตรวจหาหมายเลขไอพีของผู้รับปลายทาง เนื่องจากว่า

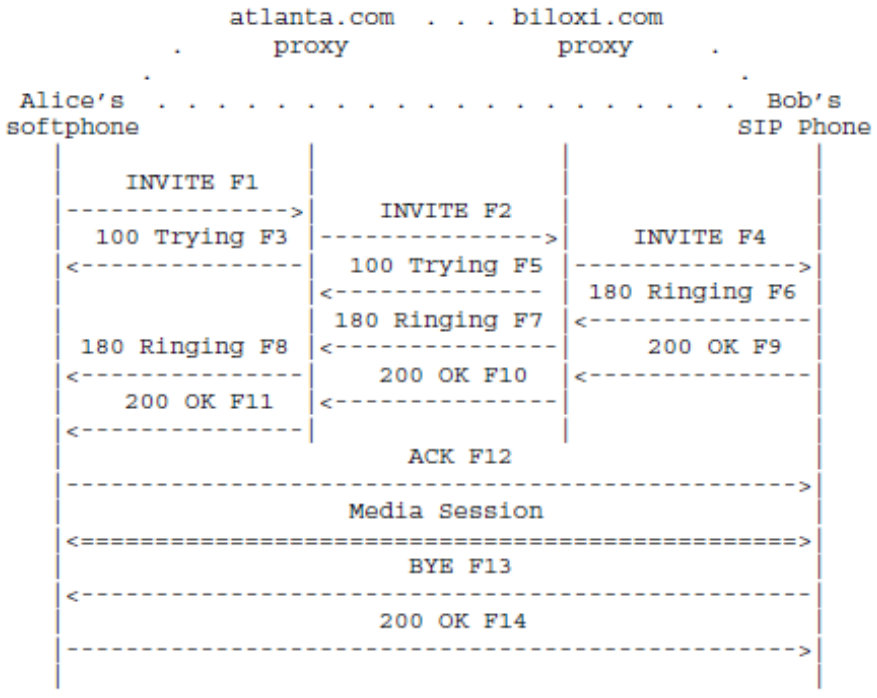
บ่อยครั้งผู้ใช้ที่เป็นเครื่องคอมพิวเตอร์จะมีหมายเลขไอพีเป็นแบบที่ไม่ตายตัว ซึ่งอาจจะได้รับมาจากการทำงานของเครื่องแม่ข่ายดีเฮชซีพี (DHCP Server) หรือผู้ใช้งานอาจมีอุปกรณ์หลายแบบที่สามารถทำงานบนเครือข่ายไอพี (โทรศัพท์มือถือ คอมพิวเตอร์พกพา เป็นต้น) ซึ่งแต่ละอุปกรณ์ก็มีหลายเลขไอพีของตัวเอง

- จัดเตรียมกลไกในการจัดการการโทร เช่น การเปลี่ยนวิธีการเข้ารหัสของข้อมูลระหว่างการโทร การเชิญผู้อื่นเข้าร่วมระหว่างการโทร การโอนย้ายการโทร การถือสายคอย เป็นต้น

อย่างไรก็ตาม ซิพไม่ได้เป็นโปรโตคอลที่สามารถทำให้เกิดบริการสื่อประสมได้ด้วยตัวเอง ดังนั้นจำเป็นที่จะต้องมีโปรโตคอลอื่นๆประกอบด้วยเช่น อาร์ทีพี (RTP, Real-Time Transport Protocol) [7] เพื่อใช้ในการขนส่งข้อมูลแบบเรียลไทม์ และสามารถส่งข้อมูลเกี่ยวกับคุณภาพของบริการกลับมาได้ (QoS Feedback) และอาร์ทีเอสพี (RTSP, Real-Time Streaming Protocol) [8] เพื่อใช้ในการควบคุมการส่งข้อมูลสื่อตรีมมิ่ง (Streaming Media) เป็นต้น

2.2 การทำงานของซิพ

ในรูปที่ 1 แสดงถึงตัวอย่างการสร้างเซสชั่นระหว่างผู้ใช้สองคนคือ อลิซและบ็อบ โดยอลิซและบ็อบจะทำการแลกเปลี่ยนข้อความของซิพระหว่างกัน (แต่ละข้อความจะมีการใส่ป้ายตัวอักษร ‘F’และหมายเลขอ้าอิง) โดยสมมติว่า อลิซใช้งานแอพพลิเคชั่นอยู่บนเครื่องคอมพิวเตอร์ ต้องการจะโทรหาบ็อบซึ่งทำงานอยู่บนโทรศัพท์ ที่รองรับการทำงานของซิพ การทำงานของทั้งสองคนจะมีการโทรผ่านเครือแม่ข่ายตัวแทนซิพ (SIP Proxy Server) ของตัวเอง



รูปที่ 1. ตัวอย่างการสร้างเซสชั่นของซิพ (นำมาจากเอกสาร RFC3261[6]

จากรูปที่ 1 อลิสทำการโทรหาบ็อบ เนื่องจาก ซอฟท์โฟน (Softphone) ไม่รู้ตำแหน่งที่อยู่ของบ็อบ หรือตำแหน่งเครื่องแม่ข่ายซิพในโดเมนของ Biloxi.com ได้ ดังนั้น ซอฟท์โฟน จึงส่งข้อความ INVITE ไปยังเครื่องแม่ข่ายซิพของตัวเองที่อยู่ในโดเมน Atlanta.com จากนั้น เครื่องแม่ข่ายจะทำหน้าที่เป็นตัวแทนในการส่งข้อความ INVITE ที่ได้รับไปยังจุดหมายต่อไป และส่งข้อความตอบกลับเป็น 100 TRYING กลับไปยังซอฟท์โฟนของอลิซ การตอบกลับเป็น 100 TRYING แสดงว่าได้มีการรับข้อความ INVITE แล้วและเครื่องแม่ข่ายตัวแทนได้ทำงานในการส่ง INVITE ต่อไปยังจุดหมายแล้ว เมื่อเครื่องแม่ข่ายตัวแทนในโดเมน Biloxi.com ได้รับข้อความ INVITE แล้วจะทำการส่งข้อความ INVITE ต่อไปยังจุดหมายปลายทางที่ระบุไว้ในข้อความ ในตัวอย่างนี้คือเครื่องโทรศัพท์ของบ็อบ จากนั้นจะตอบสนองกลับไปยังเครื่องแม่ข่ายตัวแทนที่โดเมน Atlanta.com ด้วยการส่งข้อความ 100 TRYING เมื่อบ็อบได้รับข้อความ INVITE แล้วจะมีการเตือนว่ามีการโทรเข้า (เพื่อว่าบ็อบสามารถตัดสินใจได้ว่าจะรับการโทรนี้หรือไม่) โดยเครื่องซิพโฟนของบ็อบจะตอบกลับด้วยการส่งข้อความ 180 RINGING เมื่อเครื่องแม่ข่ายตัวแทนของบ็อบได้รับข้อความก็จะส่งต่อไปยังเครื่องแม่ข่ายตัวแทนของอลิซ จากนั้น เครื่องแม่ข่ายตัวแทนของอลิสก็จะส่งข้อความต่อไปยังซอฟท์โฟน ของอลิซ เมื่อซอฟท์โฟนของอลิสได้รับ 180 RINGING แล้วก็จะมีสัญญาณเตือน (อาจเป็นข้อความหรือเสียงสัญญาณรอสาย) บนซอฟท์โฟนเพื่อให้อลิซทราบ ในขณะเดียวกันถ้าบ็อบยกหูโทรศัพท์ ก็จะมีการส่งข้อความ 200 OK ไปยังเครื่องแม่ข่ายตัวแทนของบ็อบ แล้วข้อความนี้ก็จะถูกส่งต่อไปยังเครื่องแม่ข่ายตัวแทนของอลิซจนกระทั่งถึงเครื่องซอฟท์โฟนของอลิซ เมื่อเครื่องซอฟท์โฟนของอลิซได้รับข้อความ 200 OK แล้วจะทำการหยุดสัญญาณรอสาย และจะตอบกลับด้วยข้อความ ACK ไปยังเครื่องโทรศัพท์ซิพของบ็อบโดยตรง (เนื่องจากกระบวนการที่ผ่านมาโทรศัพท์ของทั้งสองได้เรียนรู้ข้อมูลตำแหน่งที่อยู่ซึ่งกันและกันเป็นที่เรียบร้อย) กระบวนการสร้างเซสชั่นจึงเสร็จสมบูรณ์เป็นที่เรียบร้อย ข้อมูลสื่อประสมสามารถเริ่มต้นการถ่ายโอนซึ่งกันและกันได้ โดยสรุปจะเห็นได้ว่ากระบวนการติดตั้งเซสชั่นนี้เป็นกระบวนการโต้ตอบแบบ 3 ทาง (3 Way Handshaking) กล่าวคือผู้เริ่มสร้างเซสชั่นต้องมีการส่งข้อความ INVITE จากนั้น รอการตอบกลับด้วยข้อความ 200 OK และผู้เริ่มสร้างเซสชั่นตอบรับด้วยข้อความ ACK อีกครั้งหนึ่ง และเมื่อบ็อบวางหูโทรศัพท์ จะมีการยกเลิกเซสชั่นการทำงานโดยโทรศัพท์ของบ็อบจะส่งข้อความ BYEไปหาอลิซ เมื่ออลิซได้รับข้อความ BYE แล้วจะตอบกลับด้วยข้อความ 200 OK ไปหาบ็อบ เป็นการสิ้นสุดเซสชั่นการทำงาน

3. ภัยคุกคามและช่องโหว่ ของวีโอไอพี (Threats and Vulnerabilities)

จากหัวข้อที่ 2 ที่อธิบายถึงของการทำงานของซิพ จะเห็นได้ว่า โครงสร้างการทำงานของซิพไม่ได้ถูกออกแบบมาเพื่อเน้นเรื่องความมั่นคงปลอดภัยของผู้ใช้งานเช่น ไม่มีการตรวจสอบตัวตนที่แท้จริงของผู้ใช้ หรือ การเข้ารหัสลับของข้อมูลเสียง เป็นต้น ซึ่งนำไปสู่ช่องทางที่เสี่ยงต่อการโจมตีของผู้ไม่หวังดี ดังตัวอย่างต่อไปนี้

- การแอบดักฟังข้อมูล (Eavesdropping) ก็คือการที่ผู้โจมตี ทำการแอบฟังข้อมูลเสียงที่ส่งผ่านระบบอินเตอร์เน็ต เนื่องจากว่าพื้นฐานการทำงานโดยปกติแล้วจะไม่มีการเข้ารหัสลับ (Encryption) ดังนั้นผู้ที่แอบฟังก็สามารถแปลความหมายข้อมูลเสียงได้ ถึงแม้ว่าในข้อกำนดอาร์เอฟซี 3261 [6] อนุญาตให้มีการส่งโดยการทำงานของ TLS (Transport Layer Security) ได้ก็ตาม แต่ก็ไม่เป็นที่นิยมใช้ในระบบทั่วไปเนื่องจากเครื่องแม่ข่ายตัวแทนจะต้องทำงานหนักมากกว่าปกติในการรองรับจำนวนผู้ใช้จำนวนมาก
- การปฏิเสธบริการ (Denial of Service) คือ การโจมตีเพื่อให้ระบบใช้งานไม่ได้ โดยอาจจะเป็นการโจมตีไปยังเครื่องแม่ข่ายตัวแทนซิพที่ให้บริการอยู่ เช่น การส่งข้อความปกติ (เช่น INVITE) ของการทำงานซิพ หรือ ข้อความอื่นๆที่ไม่ใช่การทำงานของซิพจำนวนมากไปยังเครื่องแม่ข่ายตัวแทน ซึ่งอาจทำให้เครื่องแม่ข่ายไม่สามารถตอบสนองกับการทำงานที่เป็นปกติได้ อย่างไรก็ตามปัญหานี้ได้มีคำแนะนำไว้ใน [6] โดยจะต้องใช้อุปกรณ์เครือข่ายอื่นๆ เช่น ไฟร์วอลล์ (Firewall) เป็นต้น รวมถึงการกำหนดนโยบายต่างๆ ซึ่งผู้ดูแลระบบต้องมีความรู้แลเข้าใจอย่างดี จึงสามารถป้องกันการโจมตีได้

- วิชชิ่ง (Vishing) [9] เป็นการใช้งานการโทรศัพท์ผ่านระบบอินเตอร์เน็ต เพื่อทำวิศวกรรมทางสังคม (Social Engineering) ในหลอกเหยื่อ (Victim) เพื่อให้ข้อมูลที่เป็นส่วนตัว การเงิน และข้อมูลความลับอื่นๆ โดยคำว่า vishing มาจากคำว่า voice และ phishing โดยลักษณะการโจมตีอาจจะเกิดขึ้นในหลายรูปแบบ เช่น การส่งข้อความทางอีเมล (Email) เพื่อให้เหยื่อติดต่อกลับทางโทรศัพท์ หรือการโทรศัพท์ไปหาเหยื่อโดยตรงเป็นต้น
- การลักลอบใช้งาน (Toll Fruad) เป็นวิธีการที่ผู้โจมตีนำ รหัสลับ และชื่อผู้ใช้ ของบุคคลอื่นมาใช้ในการโทรติดต่อ ซึ่งมักจะพบในการโทรทางไกลต่างประ เทศ ซึ่งข้อมูลรหัสลับ และชื่อผู้ใช้ อาจจะได้มาจากการแอบดู (Sniffer) การทำวิศวกรรมสังคม และอื่นๆ การลักลอบใช้งานเป็นหนึ่งในการโจมตีที่เกิดบ่อยในการทำงานของวีโอไอพี
- การปลอมตัวของเครื่องแม่ข่าย (Masquerading) เมื่อผู้โจมตีสามารถที่จะปลอมตัวเป็นเครื่องแม่ข่ายตัวแทนได้ ก็จะสามารถทำให้เหยื่อส่งข้อมูลมาที่เครื่องแม่ข่ายปลอม โดยที่เครื่องแม่ข่ายปลอมอาจจะทำการจำลองการทำงานที่เสมือนมีการทำงานปกติ แต่อาจจะมีการเก็บข้อมูลความลับของผู้ใช้ไว้ ซึ่งเป็นการโจมตีในลักษณะเอ็มไอทีเอ็ม (MITM, Man in- the-Middle)
- การบุกรุกทางกายภาพ (Physical Intrusion) เป็นการคุกคามต่อภาพแวดล้อมการใช้งานของระบบ เช่น การทำให้ระบบแจ้งเตือน กล้อง กลอนประตู ไม่สามารถทำงานได้อย่างปกติ เป็นต้น และเป็นสาเหตุให้ระบบวีโอไอพี ไม่สามารถทำงานได้
- การขัดจังหวะบริการจากระบบสนับสนุน (Interruption of service) เป็นการเกิดปัญหาจากระบบสนับสนุนต่างๆที่ทำให้การทำงานของวีโอไอพีไม่สามารถดำเนินไปได้ตามปกติ เช่น ไฟฟ้าดับ ทรัพยากรของเครื่องแม่ข่ายหมดเนื่องจากมีผู้ใช้งานจำนวนมาก หรือ ลิงค์ของระบบเครือข่ายล่ม เป็นต้น
- สแปมบนระบบโทรศัพท์บนอินเตอร์เน็ต (SPIT ,Spam over Internet Telephony) เป็นการส่งข้อมูลเสียงไปหาผู้รับปลายทาง ซึ่งไม่ต้องการจะได้รับข้อมูลสียงเหล่านี้ โดยมักจะเป็นการโฆษณาสินค้าหรือการชักชวนให้ซื้อสินค้า เป็นต้น

จากภัยคุกคามที่กล่าวมานี้ หลายเรื่องไม่ได้เป็นปัญหาที่สามารถป้องกันได้โดยทางเทคนิค เช่น ภัยคุกคามที่เกี่ยวกับการทำวิศวกรรมทางสังคม เช่น วิชชิ่ง หรือ การลักลอบใช้งาน หรือภัยคุกคามจากบุกรุกทางกายภาพ เป็นต้น อย่างไรก็ตาม มีภัยคุกคามที่ได้รับความสนใจมากในงานวิจัยปัจจุบันคือเรื่องของสแปมบนระบบอินเตอร์เน็ตหรือเรียกสั้นๆว่า “สปิต” (SPIT) เนื่องจากว่า ภัยคุกคามชนิดนี้มีการใช้งานกันอย่างแพร่หลาย โดยเฉพาะเทคนิคการตลาดที่เรียกว่า การตลาดทางโทรศัพท์ (Telemarketing) ซึ่งทำให้เกิดความรำคาญต่อผู้ที่ได้รับสปิต เป็นอันมาก ในบทความนี้จะอธิบายลักษณะของ ”สปิต” และแนวทางการป้องกัน ในหัวข้อต่อไป

4. สปิต (SPIT, Spam over Internet Telephony)

4.1 ภาพรวมการทำงานของสปิต

สมิชช์ และพวก [11] ได้อธิบายความหมายของสปิตโดยสรุปคือ การโทรที่ผู้รับไม่ต้องการ หรือ ไม่อยากได้รับ หรือสปิตคือ การส่งข้อมูลเสียงหรือ การโทรครั้งละมากๆ ไปยังผู้รับ ในการเริ่มต้นของสปิต กระทำโดยการหาข้อมูลตำแหน่งซิพยูอาร์ไอ (SIP URI) ของผู้รับปลายทางหรือ เหยื่อให้ได้จำนวนมากๆ ซึ่งอาจจะทำได้โดยการสแกน ไปยังเครื่องแม่ข่ายตัวแทนซิพ เพื่อรวบรวมข้อมูลผู้ใช้ที่มีอยู่จริงนะระบบ จากนั้นผู้โจมตีสามารถสร้างการเชื่อมต่อไปหาเหยื่อได้ 2 วิธี

- ผู้โจมตีติดต่อผ่านเครื่องแม่ข่ายตัวแทนไปหาเหยื่อโดยการส่งข้อความ INVITE ผ่านเครื่องแม่ข่ายตัวแทน
- ผู้โจมตีติดต่อโดยตรงไปหาเหยื่อโดยการส่งข้อความ INVITE ไปที่เหยื่อโดยตรง

ในการโจมตีผ่านเครื่องแม่ข่ายตัวแทนผู้โจมตีจำเป็นต้องใช้ของหมายเลขซิพยูอาร์ไอ ที่เป็นแบบถาวร (Permanent SIP URI) แต่สำหรับการโจมตีไปหาเหยื่อโดยตรง ผู้โจมตีจำเป็นต้องใช้แค่ หมายเลขซิพยูอาร์ไอ ที่เป็นแบบชั่วคราวเท่านั้น เมื่อทำการเชื่อมต่อเสร็จเรียบร้อยแล้ว ก็จะทำการส่งข้อมูลเสียงไปยังปลายทางหรือเหยื่อ

4.2 การใช้งานสปิตในรูปแบบต่างๆ

ใน [13] ได้อธิบายรูปแบบต่างๆของการทำงานสปิต เป็น 4 รูปแบบดังต่อไปนี้

4.2.1 การโทรจากคอลเซนเตอร์ (Call Centres)

รูปแบบนี้มักจะเป็นการโทรเพื่อโฆษณา หรือประชาสัมพันธ์สินค้า หรือบริการเป็นหลัก โดยใช้ระบบคอมพิวเตอร์ ทำการเลือกเบอร์ของผู้ใช้ปลายทาง แล้วติดต่อไปแบบอัตโนมัติ ในกรณีที่ผู้ใช้ตอบรับจะมีการส่งต่อไปยังพนักงานขาย การโทรจากคอลเซนเตอร์แบบนี้จะมีค่าใช้จ่ายในการจ้างพนักงาน อุปกรณ์ฮาร์ดแวร์ และซอฟแวร์ที่ใช้ในการติดต่อ จำนวนการติดต่อไปภายนอกในช่วงเวลาเดียวกัน ถูกจำกัดด้วยจำนวนของพนักงานที่จะรับการตอบกลับ

4.2.2 การโทรอัตโนมัติ (Calling Bots)

การใช้ระบบคอมพิวเตอร์ทำกระบวนการทุกขั้นตอนในการทำงานโดยมีการบันทึกเสียง หรือ การตอบรับการทำงานผ่านระบบอัตโนมัติทั้งหมด ดังนั้นระบบนี้จึงสามารถสร้างการเชื่อมต่อได้เป็นจำนวนมากเมื่อเปรียบเทียบกับระบบการโทรจากคอลเซนเตอร์ เพราะไม่มีข้อจำกัดเรื่องจำนวนพนักงานที่ต้องรับการตอบกลับ

4.2.3 สปิตแบบริงโทน (Ringtone SPIT)

โทรศัพท์ที่รองรับการทำงานของวีโอไอพี บางรุ่นมีคุณสมบัติที่สามารถทำการกำหนดค่าให้สามารถรับข้อมูลส่วนหัวซิพแบบพิเศษ (Special SIP Header) ที่เรียกว่า “Alert Info” ซึ่งจะมีข้อมูลยูอาร์แอล (URL) ที่ระบุตำแหน่งที่มีการเก็บไฟล์ข้อมูลเสียงไว้บนอินเตอร์เน็ต ดังนั้นเมื่อโทรศัพท์เริ่มดังขึ้น ข้อมูลเสียงจะถูกดาวน์โหลดและเล่น ข้อความหรือโฆษณาของบริษัทต่างๆ วิธีการนี้เหยื่อไม่จำเป็นต้องมีการรับการโทร ก็สามารถได้ยินข้อความที่ส่งมาได้ อย่างไรก็ตามวิธีการนี้สามารถแก้ไขได้โดยการตั้งค่าบนเครื่องโทรศัพท์ ไม่ให้มีการดาวน์โหลดริงโทนจากอินเตอร์เน็ต

4.2.4 วิธีการผสมผสาน (Combinations)

วิธีการที่กล่าวมาอาจจะถูกนำมาใช้ร่วมกันเพื่อจุดประสงค์ที่แตกต่างกันออกไป ตามความจำเป็นและสภาพแวดล้อมของผู้ใช้งาน

โดยสรุปจากลักษณะการใช้งานและผลที่เกิดจากสปิต อาจมองว่าไม่น่าเกิดผลกระทบร้ายแรงกับเหยื่อ เพราะอาจจะเป็นแค่การสร้างความรำคาญให้แก่ผู้ที่ได้รับ แต่ในหลายครั้งมีตัวอย่างของการใช้สปิตในการก่ออาชญกรรมทางการเงินในรูปแบบทางโทรศัพท์ เช่น การหลอกเพื่อให้โอนเงินหรือทำธุรกรรมผ่านทางโทรศัพท์ เป็นต้น ดังนั้นในบทต่อไปจะกล่าวถึงแนวคิดกรอบการทำงานเพื่อป้องกันสปิต รวมถึงเกณฑ์ในการวัดประสิทธิผลของการทำงาน

5. แนวคิดกรอบการทำงานเพื่อป้องกันสปิตและเกณฑ์การวัดประสิทธิผลของการทำงาน

5.1 แนวคิดกรอบการทำงานในการสร้างวิธีการป้องกันสปิต

Quittek และคณะ [15] และ Schlegel [16] นำเสนอแนวคิดเพื่อให้เหมาะสมกับการใช้งานในทางปฏิบัติได้แนะนำแนวทางไว้ดังนี้

- โอกาสที่จะเกิดการบล็อก (Blocking) สำหรับการโทรที่ถูกต้องต้องเกิดขึ้นน้อยที่สุด
- โอกาสที่จะเกิดการบล็อก สำหรับการโทรที่เป็นสปิตต้องเกิดขึ้นมากที่สุด
- การโต้ตอบกับผู้รับปลายทาง (Callee) ต้องเกิดน้อยที่สุดระหว่างการตรวจสอบว่าเป็นสปิตหรือไม่
- การโทรที่ถูกต้องต้องได้รับความสะดวก (ไม่ควรยุ่งยากมากนัก)
- ควรจะเป็นวิธีการที่รองรับการขยายตัวของผู้ใช้ได้ (Scalable)
- ควรจะเป็นวิธีการที่มีความหยืดหยุ่นในการปรับเปลี่ยนเพื่อรองรับรูปแบบของสปิตที่อาจเปลี่ยนแปลงในอนาคต
- ควรจะเป็นวิธีการที่ประยุกต์ใช้ได้ทั่วไปในสภาพแวดล้อมต่างๆ เช่นภาษาที่ต่างกัน หรือ อื่นๆ

5.2 เกณฑ์การวัดประสิทธิผลของการทำงาน

G. F. Marias และคณะ[17] ได้อธิบายเกณฑ์ การวัดประสิทธิผลของวิธีการป้องกันสปิตไว้อย่างน่าสนใจดังต่อไปนี้

- ***ความน่าเชื่อถือ (Reliable)*** เป็นการวัดความแม่นยำในการตรวจจับ ปัญหาการผิดพลาดเชิงบวก (False Positive)

หมายถึงการวิเคราะห์ผิดพลาดจากกรณีการโทรที่ถูกต้องถูกวิเคราะห์เป็นสปิต หรือ ปัญหาการผิดพลาดเชิงลบ (False Negative) หมายถึง การวิเคราะห์ผิดพลาดจากกรณีการโทรที่เป็นสปิตถูกวิเคราะห์เป็นการโทรที่ถูกต้อง พารามิเตอร์ทั้งสองเป็นข้อมูลที่สำคัญต่อการวัดประสิทธิภาพของวิธีการป้องกันสปิตเป็นอย่างมาก

- ***เปอร์เซ็นต์ของสปิตที่มีการหลีกเหลี่ยงได้ (Percentage of SPIT calls avoided)*** โดยนับจำนวนจากสปิตจริงทำการหาสัดส่วนเปรียบเทียบกับจำนวนสปิตที่สามารถตรวจจับได้
- ***ความรวดเร็ว (Promptitude)*** เป็นการวัดความรวดเร็วของการตัดสินใจว่าการโทรเป็นสปิตหรือไม่ โดยอาจเป็นการวัดตั้งแต่เริ่มต้นร้องขอการติดต่อจนกระทั่งได้รับการตอบรับ เช่น เริ่มต้นตั้งแต่ผู้โทรส่งข้อความ INVITE จนกระทั่งได้รับข้อความ ACK เป็นต้น เนื่องจาก กระบวนการป้องกันหรือ ตัดสินใจที่ใช้เวลานาน อาจจะส่งผลในด้านความสะดวกของผู้โทรที่ถูกต้อง
- ***การรบกวนผู้ใช้ (Human Interference)*** เป็นสิ่งที่บอกถึงความยุ่งยากหรือความรำคาญที่เกิดกับผู้ใช้เนื่องจากวิธีการป้องกันสปิต โดยที่กระบวนการที่ผู้ใช้ต้องเข้าไปมีส่วนเกี่ยวข้อง กับวิธีการป้องกันด้วยควรจะมีน้อยที่สุดหรือไม่มีเลย ดังนั้นการทำโปรไฟล์ของผู้ใช้ (User Profile) อาจจะมีความจำเป็น
- ***การใช้ทรัพยากรส่วนเกินของผู้ให้บริการซิพ (Resources Overhead for the SIP Provider)*** เนื่องจากหลาย กระบวนการในการป้องกันสปิตจำเป็นที่จะต้องทำงานบนระบบที่อยู่ภายใต้การดูแลของผู้ให้บริการ เช่น การตรวจสอบตัวตน การวิเคราะห์รูปแบบของจราจร การทดสอบทัวริ่ง (Turing Test) เป็นต้น โดยกลไกเหล่านี้จะทำงานบนเครื่องแม่ข่ายตัวแทนซิพ ซึ่งต้องใช้ทรัพยากรของเครื่องแม่ข่ายต่างๆ คือซีพียู หน่วยความจำ และพื้นที่บนฮาร์ดดิสก์
- ***ค่าใช้จ่ายในรูปแบบของการเงิน (Financial Cost)*** เป็นค่าใช้จ่ายที่ผู้ให้บริการจะต้องจ่ายเพื่อเป็นค่าใช้ซอฟแวร์ หรือ ฮาร์ดแวร์ที่เกี่ยวข้องสำหรับการป้องกันสปิต ค่าอบรมพนักงาน ค่าพัฒนาระบบซอฟแวร์ หรือในบางกรณีถ้ามีการใช้ PKI (Public Key Infrastructure)[18][19] ก็จะต้องพิจารณาถึงค่าใช้จ่ายในการทำใบรับรอง
- ***ช่องโหว่ของการป้องกัน (Vulnerabilities)*** ในการสร้างวิธีการป้องกันสปิต อาจจะทำให้เกิดช่องโหว่สำหรับการโจมตีในรูปแบบอื่น หรือ สามารถเกิดผลกระทบอย่างอื่นตามมาได้เช่นกัน ตัวอย่างเช่น ระบบการใช้ชื่อเสียง (Reputation System) [20] อาจจะมีปัญหาเรื่องการสมรู้ร่วมคิดสร้างข้อมูลเทียมเพื่อให้ชื่อเสียงดี เป็นต้น
- ***ความเสี่ยงด้านความเป็นส่วนตัว (Privacy Risk)*** ข้อมูลความลับหรือข้อมูลส่วนตัวบางอย่าง อาจจะมีการใช้ในกระบวนการป้องกันหรือตรวจสอบสปิต เช่นการตรวจสอบโดยใช้ข้อมูลชีวภาพบุคคล (Biometic) [21] ดังนั้นข้อมูลเหล่านี้จำเป็นที่ผู้ให้บริการต้องมีการป้องกัน ซึ่งก็อาจถูกนำมาพิจารณาเป็นภาระเพิ่มเติมของผู้ให้บริการได้
- ***ความสามารถในการขยายตัว (Scalability)*** เป็นเกณฑ์การวัดที่สำคัญมาก เนื่องจากว่าแนวโน้มจำนวนของผู้ใช้มีการเติบโตที่สูงมากดังนั้นระบบที่ป้องกันสปิตควรจะรองรับการขยายตัวของผู้ใช้ได้ดี หรือมีข้อจำกัดในแง่ของการขยายตัวน้อยที่สุด

6. เทคนิคการป้องกันสปิต

การป้องกันสปิต มีรูปแบบต่างๆค่อนข้างหลากหลาย โดยพยายามแก้ปัญหาในด้านต่างๆ ซึ่งแต่ละวิธีการจะมีข้อดีและข้อเสียที่แตกต่างกันออกไป ใน [13] ได้จัดกลุ่มการป้องกันสปิตเป็นกลุ่มต่างๆ และวิเคราะห์จุดอ่อนของแต่ละวิธีการได้อย่างน่าสนใจดังต่อไปนี้

6.1 ลายนิ้วมือของอุปกรณ์ (Device Fingerprinting)

แนวคิดของวิธีการนี้ได้มีการนำเสนอใน [12] ผู้เขียนได้ทำการทดลองเก็บข้อมูลที่ได้จากการติดต่อระหว่างอุปกรณ์โทรศัพท์ซิพ (SIP Phone) แบบต่างๆ ทั้งแบบซอฟโฟนและเครื่องโทรศัพท์ที่เป็นฮาร์ดแวร์จริง และเมื่อทำการวิเคราะห์พบว่า อุปกรณ์โทรศัพท์ซิพแต่ละแบบ มีลักษณะของข้อมูลส่วนหัวที่ตอบสนองแตกต่างกัน ถึงแม้ว่าจะมาจากผู้ผลิตรายเดียวกันก็ตาม เช่น โทรศัพท์ซิพของบริษัทซิสโก้ ที่รุ่นไม่เหมือนกัน เป็นต้น ดังนั้นผู้เขียนสรุปว่าอุปกรณ์โทรศัพท์ซิพทุกแบบจึงมีลักษณะเฉพาะตัว ที่สามารถใช้บ่งบอกว่าการส่งข้อความมาต่างๆมาจากอุปกรณ์โทรศัพท์ซิพแบบใด ผู้เขียนได้นำเสนอลักษณะการทำงานใน [12] 2 แบบ คือลักษณะพาสซีฟ (Passive) และ แอกทีฟ (Active) การทำงานแบบพาสซีฟ เป็น

การทำงานที่ใช้ข้อมูลส่วนหัวของข้อความ INVITE ที่เกิดจากกระบวนการสร้างเซสชั่นปกติ นำมาเปรียบเทียบกับข้อมูลส่วนหัวที่เป็นของโทรศัพท์ซิพที่ใช้งานปกติ (ไม่ใช่เครื่องที่สร้างสแปม) ถ้าข้อมูลส่วนหัวไม่ตรงกับรายการที่เป็นปกติ ก็จะถือว่าเครื่องดังกล่าวเป็นเครื่องที่สร้างสแปม ในขณะที่การใช้งานแบบแอกทีฟ นั้นเครื่องแม่ข่ายตัวแทนหรือ อุปกรณ์ไฟร์วอลล์สำหรับป้องกันจะส่งข้อมูลที่เป็นมาตรฐานปกติ (Standard compliant) หรือ ข้อมูลที่ไม่ได้เป็นมาตรฐานในรูปแบบการใช้ OPTIONS (Non-compliant OPTIONS) ไปติดต่อกับอุปกรณ์โทรศัพท์ซิพ แล้วตรวจสอบข้อมูลส่วนหัวของการตอบกลับเพื่อพิจารณาว่าเครื่องใดที่เป็นเครื่องที่สร้างสแปม

จุดด้อยของวิธีการใช้ลายนิ้วมืออุปกรณ์คือ การถูกปลอมแปลงลายนิ้วมือของอุปกรณ์ได้ไม่ยาก และการเก็บรวบรวมลายนิ้วมือของอุปกรณ์แต่ละชนิดเป็นภาระของผู้ดูแลระบบที่ใช้วิธีการนี้ ซึ่งอาจส่งผลต่อในแง่การรองรับการขยายตัวของผู้ใช้

6.2 การใช้ไวท์ลิส, แบล็กลิส, เกรย์ลิส (White Lists, Black Lists, Grey Lists)

ใน [13][14] มีการนำเสนอการทำงานของไวท์ลิสดังนี้

ผู้ใช้แต่ละรายมีไวท์ลิส หรือรายการที่เป็นที่ไว้วางใจ (Trust) โดยถ้าผู้โทรที่อยู่ในไวท์ลิสจะสามารถติดต่อไปยังภายนอกได้ (โทรออกได้) ส่วนผู้ใช้ที่ไม่ได้อยู่ในไวท์ลิสจะไม่สามารถโทรออกได้ และข้อมูลไวท์ลิสของผู้ใช้แต่ละคนสามารถกระจายไปยังผู้อื่นได้ แต่ต้องมีกลไกพิเศษเพิ่มเติม ในการตรวจสอบว่าเป็นไวท์ลิสของบุคคลอื่นหรือไม่ ในกรณีที่เป็นแบล็กลิส จะตรงกันข้ามกับไวท์ลิสกล่าวคือ ถ้าผู้ใช้ใดอยู่ในแบล็กลิสถือว่าเป็นผู้สร้างสแปม (Spammer) ดังนั้นจะไม่สามารถโทรติดต่อภายนอกได้ แบล็กลิสจะสามารถถูกกระจายไปยังผู้ใช้อื่นได้เช่นกัน การใช้งานเกรย์ลิส มีลักษณะดังนี้ ตอนเริ่มต้นของการร้องขอเพื่อโทรออกจากผู้ที่ไม่ได้อยู่ในไวท์ลิส จะถูกปฏิเสธและจะถูกใส่ลงไปในเกรย์ลิส จากนั้นอาจจะมีการทำงานอะไรบางอย่างเพื่อพิสูจน์ว่าไม่ใช่สปิต จึงจะสามารถโทรออกไปยังภายนอกได้ เช่นใน [22] ทำการทดสอบโดยทัวริ่ง (Turing Test) ถ้าผ่านก็จะสามารถโทรออกได้แล้วนำหมายเลขของผู้ใช้บรรจุในไวท์ลิส และถ้าไม่ผ่านก็จะนำหมายเลขผู้ใช้บรรจุไว้ในแบล็กลิส เป็นต้น

จุดด้อยของวิธีการนี้ คือ ไม่สามารถใช้กับการโทรที่ไม่ผ่านเครื่องแม่ข่ายตัวแทนของซิพ ส่วนในกรณีที่การโทรต้องติดต่อกับเครื่องแม่ข่ายตัวแทนของซิพ จะมีจุดอ่อนคือ กระบวนการได้มาของไวท์ลิสและแบล็กลิสที่มีความถูกต้อง นอกจากนั้นการปลอมแปลงหมายเลขผู้ใช้ที่อยู่ในไวท์ลิสเป็นเรื่องที่สามารถเกิดขึ้นได้

6.3 การใช้ระบบชื่อเสียง (Reputation System)

ใน [14][23] ได้อธิบายการทำงานของกลไกชื่อเสียงไว้ดังนี้ ภายหลังจากที่ผู้รับได้รับสายการโทรแล้ว ผู้รับสามารถกำหนด ค่าชื่อเสียง (Reputation Value) ของผู้โทรได้ว่าเป็นสปิตเตอร์ (Spitter) หรือไม่ ซึ่งค่าดังกล่าวนี้จะถูกนำมาใช้ในการโทรครั้งต่อไปของผู้โทร ซึ่งอาจจะนำไปใช้ร่วมกับวิธีการเกรย์ลิส เพื่อสร้างวิธีการตัดสินใจที่ดีขึ้น โดยใน [23] ได้แสดงการส่งข้อมูลป้อนกลับ สามารถกระทำได้ 2 รูปแบบ คือ ผู้รับมีการลงทะเบียนเพื่อส่งข้อมูลกลับให้กับระบบ โดยใช้เป็นกระบวนการแยกออกจากกลไกปกติของซิพ โดยอาจทำงานผ่านข้อความ NOTIFY เพื่อแจ้งว่าผู้โทรเป็นสปิตเตอร์หรือไม่ และอีกวิธีการหนึ่งคือการใช้ข้อมูลส่วนหัวเพิ่มเติมในข้อความ BYE ที่เป็นกลไกการทำงานปกติของซิพ เพื่อส่งข้อมูลกลับจากผู้รับ ระบบ ชื่อเสียงสามารถประยุกต์ใช้ได้ทั้งแบบชื่อเสียงด้านดี (Positive Reputation) และชื่อเสียงด้านร้าย (Negative Reputation) นอกเหนือจากการให้ผู้รับปลายทางเป็นคนป้อนข้อมูลกลับ ใน [24] มีวิธีการประเมินค่าชื่อเสียงโดยวิธีการเชิงสถิติ ซึ่งคำนวณจากข้อมูลหลายชนิด เช่น จำนวนครั้งของผู้ใช้ที่ปรากฏในแบล็กลิส จำนวนครั้งการโทร ความยาวของการโทร เป็นต้น

จุดด้อยของระบบชื่อเสียงคือ การที่ผู้รับอาจจะมีการร่วมมือกับผู้โจมตี ส่งข้อมูลที่เป็นอย่างที่ผู้โจมตีต้องการได้ หรือการปลอมแปลงส่วนหัวของข้อมูลซิพที่ใช้ในการส่งข้อมูลกลับไปยังระบบ หรือในการเก็บสถิติของข้อมูลการโทรเพื่อนำมาวิเคราะห์ชื่อเสียงก็มีโอกาสที่จะเกิดการวิเคราะห์ผิดพลาดที่สูง

6.4 การทดสอบทัวริ่ง และการคำนวณแก้ปัญหา (Turing Test and Computational Puzzle)

การทดสอบของทัวริ่งเป็นวิธีการที่ใช้แนวคิดการทำงานของแคบช่า (CAPTCHA, Completely Automated

Public Turing test to tell Computers and Human Apart) โดยมีสมติฐานว่าสปิต เกิดมาจากระบบการโทรอัตโนมัติ ซึ่งไม่ใช่มนุษย์ ดังนั้น เมื่อเริ่มมีการขอขอสร้างการเชื่อมต่อ ระบบป้องกันจะยังไม่ทำการส่งข้อความ INVITE ไปยังปลายทาง แต่จะมีการ ส่งคำถามด้วยเสียง เพื่อให้ผู้โทรตอบก่อน ถ้าเป็นมนุษย์จะสามารถตอบได้ ในขณะที่ถ้าเป็นการโทรด้วยระบบอัตโนมัติจะไม่สามารถตอบได้ วิธีการดังกล่าวได้มีการนำเสนอไว้ใน [26] นอกจากนั้นใน [25][22] ได้มีการนำผลลัพธ์จากการทดสอบทัวริ่งไปใช้ในการสร้างไวท์ลิส

สำหรับการคำนวนเพื่อแก้ปัญหา เป็นแนวคิดที่คล้ายคลึงกับการทดสอบทัวริ่ง แต่จุดประสงค์ต่างกัน ใน [27] อธิบายการทำงานไว้ดังนี้ เมื่อมีการส่งข้อความ INVITE มายังเครื่องแม่ข่ายของซิพ เครื่องแม่ข่ายจะทำการส่งปัญหาไปยังผู้โทร จากนั้นผู้โทรจะส่งข้อความร้องขอคำตอบมาที่เครื่องแม่ข่าย แล้วเครื่องแม่ข่ายจะส่งวิธีการแก้ปัญหาไปให้ การแก้ปัญหาจะใช้การคำนวณทางคณิตศาสตร์ จะเห็นได้ว่าวิธีการนี้ไม่ได้มีจุดมุ่งหมายเพื่อขจัดสปิต แต่เป็นการเพิ่มภาระให้กับซีพียูของผู้โทร ทำให้ผู้โทรลดการโทรที่ไม่จำเป็นลง

จุดด้อยของวิธีการนี้คือ ถ้าการทำทดสอบทัวริ่งไม่ซับซ้อนอาจจะถูกผู้โจมตีใช้เครื่องมือวิเคราะห์เสียงแล้วสร้างคำตอบไว้ล่วงหน้าได้ ขณะที่กรณีของการคำนวณแก้ปัญหาไม่สามารถป้องกันสปิตได้เพราะผู้โจมตีต้องการแค่ระบบที่มีกำลังของซีพียูที่มากพอ ซึ่งก็เป็นเรื่องปกติที่ผู้โจมตีจะใช้คอมพิวเตอร์ตั้งโต๊ะ (Desktop Computer) ที่มีประสิทธิภาพสูง ผลกระทบที่เกิดขึ้นกลับไปปรากฏที่ผู้ใช้งานที่ถูกต้องทั่วไป ที่จะเกิดการเชื่อมต่อที่ช้าลง พลังงานของอุปกรณ์ใช้มากขึ้น (ในกรณีที่เป็นอุปกรณ์แบบเคลื่อนที่ได้)

6.5 การจ่ายเงินตามความเสี่ยง (Payment at Risk)

แนวคิดของวิธีการนี้คือการเพิ่มค่าใช้จ่ายให้กับผู้โทรที่อาจเป็นสปิต โดย [14] อธิบายวิธีการนี้ไว้ดังต่อไปนี้ เมื่อผู้โทรต้องการโทรไปยังปลายทางจะต้องมีการจ่ายเงินค่าโทรไปให้กับผู้รับปลายทาง เมื่อผู้รับปลายทางยืนยันกลับว่าไม่ใช่สปิต ผู้โทรจะได้รับเงินจำนวนนั้นคืน แต่ถ้าผู้โทรเป็นสปิต ก็อาจจะมีมาตรการด้านราคาเช่น ถูกปรับเงินขึ้น เป็นต้น วิธีการนี้อาจจะนำไปใช้งานร่วมกับไวท์ลิส โดยที่ผู้ที่ไม่ได้อยู่ในไวท์ลิสจะต้องมีการจ่ายเงินเมื่อต้องการจะติดต่อกับผู้รับปลายทาง จุดด้อยของวิธีการจ่ายเงินตามความเสี่ยงคือ ถ้าวิธีการนี้มีการใช้ร่วมกับไวท์ลิส ผู้โจมตีสามารถปลอมหมายเลขของผู้ใช้ที่อยู่ในไวท์ลิสได้ ทำให้ไม่ต้องจ่ายเงินล่วงหน้า ในกรณีทั่วไป ผู้โจมตีอาจจะสร้างการโทรที่เป็นปกติไปหาผู้ใช้ปลายทางเพื่อให้หมายเลขของผู้โทรเข้าไปอยู่ในไวท์ลิส จากนั้นจึงทำการสร้างสปิตขึ้นมาทำให้ม่ต้องจ่ายเงินล่วงหน้าเช่นกัน นอกเหนือจากช่องโหว่ในการโจมตีแล้ว วิธีการนี้จำเป็นต้องมีระบบการจ่ายเงินมาร่วมด้วยซึ่งอาจจะทำให้เกิดความไม่สะดวกกับผู้ใช้บริการและเป็นภาระเพิ่มเติมของผู้ให้บริการ

7. บทสรุป

บทความนี้เป็นการบรรยายให้เห็นถึงเหตุผลของการใช้งานอย่างแพร่หลายของวีโอไอพีในปัจจุบัน รวมไปถึงโครงสร้างพื้นฐานการทำงานของวีโอไอพี ที่เกิดจากโปรโตคอลซิพ ซึ่งเป็นโปรโตคอลหลักสำหรับวีโอไอพี จากนั้นทำการแสดงภัยคุกคามและช่องโหว่ต่างๆที่เกิดขึ้นบนระบบวีโอไอพี อย่างไรก็ตามภัยคุกคามที่เกิดขึ้นมาจากการทำวิศวกรรมทางสังคม ซึ่งการป้องกันในเชิงเทคนิคสามารถทำได้ยาก การป้องกันภัยคุกคามประเภทนี้ต้องสร้างความรู้และความเข้าใจให้กับผู้ใช้งานให้มากที่สุด แต่ภัยคุกคามที่ในบทความนี้ได้ให้ความสนใจคือ สแปมบนการโทรศัพท์บนอินเตอร์เน็ตหรือเรียกสั้นๆว่า *สปิต* เพราะเป็นภัยคุกคามที่เกิดขึ้นมากที่สุดในระบบวีโอไอพี ถึงแม้จะสร้างผลเสียหายน้อย แต่ได้สร้างความรำคาญให้กับผู้รับปลายทางมาก ในบทความได้แสดงกรอบแนวคิดเพื่อใช้ป้องกันสปิต ที่มีนักวิจัยได้นำเสนอขึ้นเพื่อใช้ป้องกันว่าควรเป็นอย่างไร รวมถึง เกณฑ์การประเมินเพื่อให้ผู้อ่านได้ทราบถึงปัจจัยต่างๆที่ควรนำมาพิจารณาในการสร้างวิธีการป้องกันสปิต และได้บรรยายถึงวิธีการป้องกันสปิตแบบต่างๆ พร้อมแสดงจุดอ่อนของวิธีการต่างๆไว้

สุดท้ายจะเห็นว่าวิธีการป้องกันต่างๆ ยังมีข้อด้อยที่สามารถนำไปพัฒนาวิธีการหรือกลไกในการป้องกันสปิตให้มีความสามารถมากขึ้นในอนาคตต่อไป

เอกสารอ้างอิง

[1] M. Gori and F. Scarselli, “Are Multilayer Perceptron Adequate for Pattern Recognition and Verification?”, *IEEE Transactions onPattern*

Analysis and Machine Intelligence, Vol. 20, No. 11, November 1998. pp. 1121-1132

[2] http://www.totnetcall.com/

[3] http://www.truenettalk.com/th/products/international_rate.html

[4] http://www.contactcenter.cattelecom.com/thai/oversea/cat009_info.asp

[5] http://www.tot.co.th/index.php?option=com_linkcontent&categoryid=89&Itemid=127&lang=th

[6] J. Rosenberg, et al., "Session Initiation Protocol", RFC 3261, June 2002.

[7] Schulzrinne, H., Casner, S., Frederick, R. and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", RFC 1889, January 1996

[8] Schulzrinne, H., Rao, R. and R. Lanphier, "Real Time Streaming Protocol (RTSP)", RFC 2326, April 1998.

[9] The vishing guide, IBM Global Technology Services, May 2007

[10] Keromytis, A. "A Comprehensive Survey of Voice over IP SecurityResearch",IEEE COMMUNICATIONS SURVEYS & TUTORIALS Journal

[11] Dr. Andreas U. Schmidt1, Nicolai Kuntze1, Rachid El Khayar, "SPAM OVER INTERNET TELEPHONY AND HOWTO DEAL WITH IT" ,7th annual Conference Information Security South Africa (ISSA 2008), South Africa, 7 -9 July 2008.

[12] H. Yany, K. Sripanidkulchaiz, H. Zhangy, Z. Shaez and D. Saha," Incor-porating Active Fingerprinting into SPIT Prevention Systems", 2007.

[13] M. Hansen, M. Hansen, J. M oller, T. Rohwer, C. Tolkmit and H. Waack, "Developing a Legally Compliant Reachability Management System as a Countermeasure against SPIT", 2007.

[14] J. Rosenberg, C. Jennings, RFC 5039 - The Session Initiation Protocol(SIP) and Spam, IETF, 2008.

[15] Juergen Quittek, Saverio Niccolini, Sandra Tartarelli, and Roman Schlegel, NEC Europe Ltd."On Spam over Internet Telephony (SPIT) Prevention",IEEE Communication Magazine, 2008,pp.80-86

[16] Roman Schlegel, Saverio Niccolini, Sandra Tartarelli and Marcus Brunner, "SPam over Internet Telephony (SPIT) Prevention Framework", *IEEE GLOBECOM 2006*

[17] G. F. Marias S. Dritsas M. Theoharidou J. Mallios D. Gritzalis, " SIP Vulnerabilities and Anti-SPIT Mechanisms Assessment", ICCCN 2007. Proceedings of 16th International Conference on Computer Communications and Networks, 2007.pp 597-604

[18] N. Croft, M. Olivier, "A Model for Spam Prevention in Voice over IP Networks using Anonymous Verifying Authorities," in Proc. of the 5th Annual Information SecuritySouth Africa Conference (ISSA 2005), South Africa, July 2005

[19] J. Peterson, and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol", RFC4474, August 2006.

[20] H. Tschofenig, R Falk, J. Peterson, et al., "Using SAML to Protect the Session Initiation Protocol", IEEE Network, 20 (5), pp. 14-17 September/October 2006.

[21] R. Baumann, S. Cavin, S. Schmid, "Voice Over IP – Security and SPIT", Swiss Army, FU Br 41, KryptDet Report, Univ. of Berne, September 2006.

[22] S.Wiwatpinyo, W.lilakiatsakun, "Enhanced VOIP ANTI-SPIT Mechanism Based on Modular Design, in Proc.of the 3rd ECTICARD2011,Thailand, pp 232-237.

[23] M. Stiemerling S. Niccolini, S. Tartarelli, "Requirements and methods for SPIT identification using feedbacks in SIP", Internet-draft, 2008.

[24] F. Wang, Y. Mo, B. Huang, "P2P-AVS: P2P Based Cooperative VoIP Spam Filtering", 2007.

[25] H. Tschofenig, E. Leppanen, S. Niccolini, M. Arumaithurai, "Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA) based Robot Challenges for SIP". Internet-draft, 2008.

[26] Alexander Johanson, W.lilakiatsakun, "A VOIP anti-Spam System based on Audio Turing Test Server",in Proc.of the 2rd ECTI-CARD2010,Thailand, pp 406-410.

[27] C. Jennings, "Computational Puzzles for SPAM Reduction in SIP", Internet-draft, 2008.