บทที่ 5
สรุปผล และข้อเสนอแนะ

จากการศึกษา และออกแบบระบบพิสูจน์ตัวตนด้วยเคอร์เบอรอสทำให้เข้าถึงถึงวิธีการพิสูจน์ตัวตนเพียงครั้งเดียวด้วยคอร์เบอร์รอส เพื่อเข้าใช้บริการซีเคียวเชลล์ด้วยการพิสูจน์ตัวตนเพียงครั้งเดียว ในส่วนการพัฒนาระบบตรวจจับการบุกรุกบนอุปกรณ์ฝังตัวราสเบอรี่ไพนั้นทำให้เข้าใจถึงวิธีการนำโปรแกรมสนอร์ทซึ่งเป็นโปรแกรมระบบตรวจจับการบุกรุกติดตั้งด้วยเทคนิคด็อกเกอร์ไฟล์ รวมถึงเข้าใจสถาปัตยกรรมลำดับการทำงานของเคอร์เบอรอสสำหรับการพิสูจน์ตัวตนเพียงครั้งเดียว และสนอร์ทสำหรับการตรวจจับการบุกรุก

5.1 สรุปผลดำเนินงาน

งานวิจัยนี้ได้นำเสนองานการพัฒนาระบบตรวจจับการบุกรุกบนอุปกรณ์ฝังตัวเพื่อแจ้งเตือนการบุกรุกเครื่องแม่ข่ายเคอร์เบอรอสการดำเนินงานครั้งนี้ได้ทำการทดลองแบ่งการทดลองเป็น 12 แบบการทดลอง โดยจำแนกการทดลองเป็นรูปแบบการโจมตี TCP Flood, UDP Flood, ICMP Flood รูปแบบการสื่อสารเครือข่ายภายใน เครือข่ายภายนอก และชนิดสื่อกลางการสื่อสารแบบสายไร้สาย การทดลองดังกล่าวนำมาใช้ทดสอบกับเคอร์เบอรอส เซิฟเวอร์ อุปกรณ์ฝังตัวราสเบอรี่ไพที่ติดตั้งระบบตรวจจับการบุกรุก และเซิฟเวอร์ที่ติดตั้งระบบตรวจจับการบุกรุก ซึ่งผลการทดลองบันทึกค่าทรัพยากร CPU, RAM และ Network ด้วยโปรแกรมที่เขียนมาด้วยเทคนิคเชลล์สคริป โดยบันทึกค่าทรัพยากรทุก ๆ 5 วินาที บันทึกตังแต่วินาทีที่ 0 ซึ่งเป็นวินาทีที่มีค่าทรัพยากรทำงานตามปกติจนถึงวินาทีที่ 120 ผลลัพธ์คือ การบุกรุกโจมตีแบบ TCP Flood, UDP Flood และ ICMP Flood ของเครื่องแม่ข่ายเคอร์เบอร์รอสมีค่าทรัพยากรรวมเฉลี่ย 65.08 เปอร์เซ็นต์ 44.38 เปอร์เซ็นต์ และ 41.45 เปอร์เซ็นต์ ตามลำดับ การบุกรุกโจมตีทางชนิดสื่อกลางการสื่อสารแบบสาย และไร้สายของเครื่องแม่ข่ายเคอร์เบอร์รอสมีค่าทรัพยากรรวมเฉลี่ย 60.20 เปอร์เซ็นต์ และ 40.40 เปอร์เซ็นต์ ตามลำดับ การบุกรุกโจมตีรูปแบบการสื่อสายภายใน และภายนอกของเครื่องแม่ข่ายเคอร์เบอร์รอสมีค่าทรัพยากรรวมเฉลี่ย 52.33 เปอร์เซ็นต์ และ 48.27 เปอร์เซ็นต์ ตามลำดับ การทำงานการตรวจจับการบุกรุกของอุปกรณ์ฝังตัวเมื่อมีการโจมตีรูปแบบ TCP Flood, UDP Flood และ ICMP Flood มีค่าทรัพยากรรวมเฉลี่ย 35.35 เปอร์เซ็นต์ 34.48 เปอร์เซ็นต์ และ 28.48 เปอร์เซ็นต์ ตามลำดับ การทำงานการตรวจจับการบุกรุกของอุปกรณ์ฝังตัวด้วยชนิดสื่อกลางการสื่อสารแบบสาย และไร้สายมีค่าทรัพยากรรวมเฉลี่ย 45.59 เปอร์เซ็นต์ และ 19.95 เปอร์เซ็นต์ ตามลำดับ การทำงานการตรวจจับการบุกรุกของ

อุปกรณ์ฝังตัวด้วยรูปแบบการสื่อสารภายใน และภายนอก มีค่าทรัพยากรรวมเฉลี่ย 35.31 เปอร์เซ็นต์ และ 30.23 เปอร์เซ็นต์ ตามลำดับ ผลการทำงานของเคอร์เบอรอส เซิฟเวอร์ ที่ติดตั้งระบบตรวจจับการบุกรุกมีค่าทรัพยากร CPU, RAM และ Network เฉลี่ยเป็น 30.80 79.43 และ 57.51 ตามลำดับ ผลการทำงานของเคอร์เบอรอส เซิฟเวอร์ ที่แยกการติดตั้งระบบตรวจจับการบุกรุกไปยังราสเบอรี่ไพมีค่าทรัพยากร CPU, RAM และ Network เฉลี่ยเป็น 24.02 69.37 และ 57.51 ตามลำดับ

การทดลองได้ทำตามวัตถุประสงค์ คือ การใช้งานกระบวนการพิสูจน์ตัวตนด้วยเคอร์เบอรอส มีกระบวนการที่ไม่ซับซ้อนสามารถเข้าใช้บริการซีเคียวเชลล์ผ่านระบบเครือข่ายได้ การใช้งานระบบตรวจจับการบุกรุกสำมารใช้ผ่านระบบเครือข่ายได้อย่างราบรื่น สามารถออกแบบ และพัฒนาระบบตรวจจับการบุกรุกในการเข้าใช้บริการ ในระบบเครือข่ายบนอุปกรณ์ฝังตัวราสเบอรี่ไพได้

5.2 การวิเคราะห์ผลการทดลอง

จากผลการทดลองในบทที่ 4 ได้แบ่งการทดลองเป็น 12 แบบการทดลอง โดยจำแนกการทดลองโดยจำแนกการทดลองเป็นรูปแบบการโจมตี TCP Flood, UDP Flood, ICMP Flood กำหนดให้ทุกรูปแบบการโจมตีมีค่าแพ็กเก็ตที่ 1448 ไบต์ เพื่อให้มีค่าแพ็กเก็ตที่เท่ากันเนื่องจากโปรแกรม LOIC ที่มีการใช้รูปแบบการโจมตีแบบ TCP Flood และ UDP Flood ปรับค่าแพ็กเก็ตให้มีประสิทธิภาพการโจมตีที่รุนแรงที่สุดเป็น 1448 ไบต์ ทำให้การใช้งานโปรแกรมที่มีรูปแบบการโจมตี ICMP Flood มีขนาดแพ็กเก็ตเป็น 1448 ไบต์ด้วย การจำแนกต่อไป คือ รูปแบบการสื่อสารเครือข่ายภายใน เครือข่ายภายนอก เพราะการโจมตีนั้นมีได้ทุกสถาณที่ที่มีการเชื่อมต่อหากันได้ ฉะนั้นจึงมีการติดต่อระหว่างเครือข่ายกันด้วยแนท ส่วนชนิดสื่อกลางการสื่อสารแบบสาย ไร้สาย เป็นการใช้งานในความเป็นจริงมีการใช้งานได้ทั้งสายแลน และแบบไวไฟ ผลการทดลองการบุกรุกโจมตีแบบ TCP Flood ของเครื่องแม่ข่ายเคอร์เบอร์รอสมีค่าทรัพยากรรวมเฉลี่ยมีความรุนแรงมากที่สุดคิดเป็น 1.46 และ 1.57 เท่าของ UDP Flood และ ICMP Flood ตามลำดับ เพราะการใช้การโจมตีรูปแบบ TCP Flood นั้นทำให้ CPU มีการประมวลผลนานขึ้นเนื่องจากกระบวนการ SYN-ACK ของ TCP Flood ที่มีการส่งแพ็คเก็ตหลายครั้งเป็นจำนวนมาก เมื่อมีการประมวลผลที่ช้าทำให้มีการใช้ RAM เพิ่มขึ้นด้วย เพราะแพ็คเก็ตที่เข้ามาจะถูกเก็บไว้ที่ RAM ก่อนที่ให้ CPU ทำการอ่านข้อมูลแล้วทำการลบข้อมูลจาก RAM ออกไป ผลการบุกรุกโจมตีทางชนิดสื่อกลางการสื่อสารแบบสายของเครื่องแม่ข่ายเคอร์เบอรอสมีค่าทรัพยากรรวมเฉลี่ยสูงสุดคิดเป็น 1.49 เท่า ของชนิดสื่อกลางการสื่อสารแบบไร้สาย เพราะการเชื่อมต่อแบบสายนั้นมีการรับส่งข้อมูลได้ในเวลาเดียวกันในขณะที่แบบไร้สายจะสลับการรับส่งข้อมูลและมีขนาดแบนด์วิธเพียงกว่าแบบสายถึง 1.8 เท่า ผลการบุกรุกโจมตีรูปแบบการสื่อสายภายในของเครื่องแม่ข่ายเคอร์เบอร์รอสมีค่าทรัพยากรรวมเฉลี่ยสูงกว่าภายนอก 1.08 เท่า เพราะการติดต่อต่าง

เครือข่ายกันกล่าวคือมีการใช้เลขซับเน็ตมาร์ค (Subnet mask) ที่ต่างกันทำให้ไม่สามารถติดต่อหากันได้ แต่ด้วยความสามารถของเราท์เตอร์นั้นมีฟังก์ชันแนทซึ่งเป็นความสารถแปลงเลขซับเน็ตมาร์คให้มองเห็นกันได้ แต่ทำให้เป็นการรอบกวนการทำงานเราท์เตอร์จึงมีโอกาสสูญเสียข้อมูลที่ส่งไปบางส่วน ผลการทดลองการตรวจจับบุกรุกโจมตีแบบ TCP Flood ค่าทรัพยากรรวมเฉลี่ยคิดเป็น 1.02 และ 1.24 เท่า ของ UDP Flood และ ICMP Flood ตามลำดับ เห็นได้ว่าการตรวจจับ TCP Flood และ UDP Flood มีความแตกต่างกันไม่มากเนื่องจากข้อมูลที่แนบมานั้นมีการสุ่มข้อความใหม่อยู่เสมอ แต่ส่วนของ ICMP Flood นั้นมีการสุ่มข้อความในข้อมูลที่ส่งมาน้อยกว่าทำให้การตรวจจับการบุกรุก ICMP Flood มีการใช้ทรัพยากรน้อยที่สุด ผลการทำงานการตรวจจับการบุกรุกของอุปกรณ์ฝังตัวด้วยชนิดสื่อกลางการสื่อสารแบบสายมีค่าทรัพยากรรวมเฉลี่ยมากกว่าแบบไร้สายถึง 2.28 เท่า เนื่องจากการเชื่อมต่อแบบสายนั้นมีการรับส่งข้อมูลได้ในเวลาเดียวกันในขณะที่แบบไร้สายจะสลับการรับส่งข้อมูล โดยข้อมูลที่นำไปตรวจจับนั้นจะขึ้นอยู่กับเคอร์เบอร์รอส เซิฟเวอร์ ถูกโจมตีด้วยชนิดสื่อกลางการสื่อสารแบบไหน ผลการทำงานการตรวจจับการบุกรุกของอุปกรณ์ฝังตัวด้วยรูปแบบการสื่อสารภายในมีค่าทรัพยากรรวมเฉลี่ยมากว่าภายนอกถึง 1.16 เท่า เพราะเกิดการสูญเสียข้อมูลที่เคอร์เบอร์รอส เซิฟเวอร์ที่ถูกยิงมาจากภายนอกจาการแนทของเราท์เตอร์ ในส่วนผลการทำงานของเคอร์เบอรอส เซิฟเวอร์ ที่ติดตั้งระบบตรวจจับการบุกรุก มีค่าทรัพยากร CPU และ RAM มากกว่าเคอร์เบอรอส เซิฟเวอร์ ที่แยกการติดตั้งระบบตรวจจับการบุกรุกไปยังราสเบอรี่ไพถึง 1.28 และ 1.15 เท่าของเคอร์เบอรอส เซิฟเวอร์ ที่แยกการติดตั้งระบบตรวจจับการบุกรุกไปยังราสเบอรี่ไพ ทำให้การติดตั้งระบบตรวจจับการบุกรุกลงบนอุปกรณ์ราชเบอรี่ไพช่วยให้ลดค่าทรัพยากรที่ใช้ในเคอร์เบอรอส เซิฟเวอร์ ที่ติดตั้งระบบตรวจจับการบุกรุกได้ และไม่เป็นการรบกวนการทำงานของเคอร์เบอร์รอส เซิฟเวอร์ ในส่วน Netwrok นั้นเท่ากัน เพราะมีการเปิดใช้งานแสปนพอร์ตในสวิทช์ทำให้รับข้อมูลเหมือนกับเคอร์เบอร์รอส เซิฟเวอร์ทุกประการ โดยจะคัดลอกข้อมูลที่เคอร์เบอรอส เซิฟเวอร์ ที่รับมาทั้งหมด แต่ข้อมูลนั้นจะไม่มีผลกระทบใด ๆ ต่ออุปกรณ์ฝังตัวราสเบอรีไพ และอุปกรณ์ฝังตัวราสเบอรี่ไพสามารถใช้งานอย่างราบรื่นโดยไม่มีปัญหาใด ๆ

5.3 ปัญหาและอุปสรรคในการดำเนินงาน

5.3.1 อุปกรณ์ที่ใช้ในการทดลองมีรุ่นเก่าทำให้มีความเร็ว Network ได้เพียง 100 Mbps

5.3.2 อุปกรณ์ฝังตัวราสเบอรี่ไพมีความเร็ว Network ได้เพียง 100 Mbps โดยที่ปัจจุบันอุปกรณ์อื่น ๆ มีความเร็ว 1 Gbps

5.4 แนวทางการพัฒนางานวิจัย

5.4.1 สามารถนำไปพัฒนาต่อในการใช้งานที่มีความเร็ว Network 1 Gbps ในอุปกรณ์ฝังตัวราสเบอรี่ไพที่มาในอนาคตได้

5.4.2 เพิ่มการใช้งานการแจ้งเตือนการบุกรูปในรูปของ Web Application