บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

เนื่องด้วยปัจจุบันการขยายตัวของระบบเครือข่ายมีอัตราการเติบโตที่รวดเร็ว ซึ่งการบริการระบบเครือข่ายในปัจจุบัน มีการให้บริการหลากหลายรูปแบบให้ผู้ใช้สามารถเลือกค้นคว้า หาข้อมูลที่ต้องการจากแหล่งข้อมูลขนาดใหญ่ได้อย่างหลากหลายและรวดเร็วมากขึ้น และยังสามารถทำการติดต่อสื่อสารและการโอนย้ายข้อมูลได้อย่างอิสระ เนื่องจากความยืดหยุ่นของระบบเครือข่ายอินเทอร์เน็ตทำให้สามารถพัฒนาการให้บริการได้ง่ายกว่าเครือข่ายอื่น

ปัจจุบันระบบคอมพิวเตอร์ที่ถูกวางบนเครือข่ายมักเป็นระบบเปิดซึ่งยอมให้มีการติดต่อขอใช้งานจากระยะไกลได้ บุคคลที่ติดต่อขอใช้บริการผ่านทางเครือข่ายคอมพิวเตอร์สามารถทำการเชื่อมต่อแล้วเข้าใช้บริการผ่านเครื่องผู้ให้บริการจากตำแหน่งที่อยู่บนระบบเครือข่ายทำหน้าที่เป็นเครื่องผู้ให้บริการแก่เครื่องผู้รับบริการ เมื่อมีการขอเข้าใช้บริการมากขึ้นจากแหล่งต่าง ๆ บนเครือข่ายอินเทอร์เน็ตอาจจะมีผู้ใช้บางคนที่ไม่ประสงค์ดีบุคคลเหล่านี้อาจทำให้เกิดความเสียหายต่อเครือข่ายและองค์กรหน่วยงานต่าง ๆ ได้

องค์กรหน่วยงานต่าง ๆ โดยจึงจำเป็นต้องมีระบบตรวจจับการบุกรุก และระบบพิสูจน์ตัวตน เป็นอีกทางหนึ่งในการช่วยรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ หากเปรียบระบบเครือข่ายคอมพิวเตอร์เหมือนบ้านแล้วเคอร์เบอรอสเปรียบเสมือนประตูเข้าบ้านที่ต้องสแกนลายนิ้วมือและระบบตรวจจับการบุกรุก เปรียบเสมือนยามรักษาการณ์ภายในบ้านที่ชำนาญในการวิเคราะห์คนผ่านเข้าออกโดยดูจากลักษณะ และพฤติกรรมของบุคคลที่ไม่ประสงค์ดีหากใครมีพฤติกรรมน่าสงสัยก็จะรายงานให้ผู้ดูแลระบบทราบทันทีนับว่า ระบบตรวจจับการบุกรุกเป็นเครื่องมือสำคัญอย่างยิ่งที่จะรับมือการบุกรุกจากผู้บุกรุก

1.2 วัตถุประสงค์

1.2.1 เพื่อศึกษาและพัฒนากระบวนการของระบบป้องกันการบุกรุกเครือข่ายในการแจ้งเตือนผู้บุกรุกที่กระทำการระงับ ชะลอ หรือรบกวนต่อเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ในการรักษาความมั่นคงทางไซเบอร์ อันก่อให้เกิดผลกระทบทางสร้างสรรค์ในด้านการพัฒนาเศรษฐกิจในยุคดิจิทัล

1.2.2 เพื่อวิเคราะห์การลดโอกาสการรบกวนด้วยวีธีปฏิเสธการให้บริการ (Daniel of Service) กับเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ในการรักษาความมั่นคงทางไซเบอร์

1.2.3 เพื่อวิเคราะห์การเพิ่มประสิทธิภาพในการป้องกันการบุกรุกต่อเครื่องคอมพิวเตอร์แม่ข่ายของระบบถ่ายทอดโทรทัศน์ผ่านอินเทอร์เน็ตอันเป็นการสร้างองค์ความรู้เพื่อรองรับการก้าวสู่ประชาคมเศรษฐกิจอาเซียน (ASEAN Economic Community : AEC)

1.3 ขอบเขตของงาน

1.2.1 สามารถศึกษากระบวนการของระบบพิสูจน์ตัวตนในการเข้าใช้บริการซีเคียวเชลผ่านระบบเครือข่ายโดยใช้ระบบพิสูจน์ตัวตนแบบลงทะเบียนเพียงจุดเดียวด้วยเคอร์เบอรอส

1.2.2 สามารถศึกษากระบวนการบุกรุกเครือข่ายผ่านระบบเครือข่ายด้วยระบบตรวจจับการบุกรุกด้วยสนอร์ทได้

1.2.3 สามารถออกแบบ และพัฒนาระบบตรวจจับการบุกรุกในการเข้าใช้บริการสนอร์ทที่ใช้ในการรักษาความมั่นคงทางไซเบอร์ ในระบบเครือข่ายบนอุปกรณ์ฝังตัวราสเบอรี่ไพได้

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1.3.1 ได้รับความรู้เกี่ยวกับกระบวนการทำงานของระบบพิสูจน์ตัวตนเคอร์เบอรอส

1.3.2 สามารถนำระบบพิสูจน์ตัวตนเคอร์เบอรอสไปใช้งานได้จริง

1.3.3 ได้รับความรู้เกี่ยวกับระบบตรวจจับการบุกรุก

1.3.4 ได้รับความรู้เกี่ยวกับอุปกรณ์ฝังตัวราสเบอรี่ไพ

1.3.5 สามารถนำระบบตรวจจับการบุกรุกติดตั้งบนอุปกรณ์ฝังตัวราสเบอรี่ไพไปใช้งานได้จริง

1.5 นิยามศัพท์เฉพาะ

1.5.1 **ระบบพิสูจน์ตัวตน** (Authentication Service: AS) [1] คือ ระบบงานบริการที่ทำหน้าที่เกี่ยวกับการพิสูจน์ตัวตน และตรวจสอบสิทธิการให้บริการ จากการลงชื่อเข้าใช้

1.5.2 **เครื่องลูกข่าย** (Client) [2] คือ เครื่องคอมพิวเตอร์ หรือเครื่องลูกข่ายใด ๆ ที่ไปร้องขอบริการและรับบริการอย่างใดอย่างหนึ่งจากเครื่องแม่ข่าย

1.5.3 **อุปกรณ์ฝังตัว** (Embedded Device) [3] คือ อุปกรณ์คอมพิวเตอร์ขนาดเล็ก มีการฝังตัว เป็นเหมือนสมองกลใช้ควบคุมการทำงานในเครื่องใช้ไฟฟ้าต่าง ๆ เช่น เครื่องปรับอากาศ, เครื่องซักผ้า, เครื่องเย็บผ้า ฯลฯ

1.5.4 **ระบบตรวจจับการบุกรุก** (Intrusion Detection System: IDS) [4] คือ ซอฟแวร์หรือฮาร์ดแวร์ที่ได้รับการออกแบบมาเพื่อให้ตรวจสอบการเชื่อมต่อที่ไม่พึงประสงค์ หรือความพยายามที่จะเข้ามาทำอันตรายต่อเครือข่าย โดยผ่านระบบเครือข่าย

1.5.5 **เคอเบอร์รอส** (Kerberos) [5] คือ โปรโตคอลการพิสูจน์ตัวตนของเครือข่ายที่ออกแบบมา เพื่อให้มีการพิสูจน์ตัวตนของแอพพลิเคชั่นแบบ Client/Server (Domain) โดยใช้วิทยาการเข้ารหัสลับของคีย์ลับ

1.5.6 **ศูนย์กลางการกระจายกุญแจ** (Key Distribution Center: KDC) [6] คือกระบวนการแลกเปลี่ยน กุญแจโดยอาศัยศูนย์กลางในการแลกเปลี่ยนกุญแจในการเข้าและถอดรหัส

1.5.7 **ระบบเครือข่าย** (Network) [7] คือ การเชื่อมต่อคอมพิวเตอร์ ตั้งแต่ 2 เครื่องขึ้นไปเข้าด้วยกัน เช่น การเชื่อมต่อเครื่องคอมพิวเตอร์ภายในห้องเรียน ภายในองค์กร ระหว่าง อาคาร ระหว่างเมืองต่าง ๆ ตลอดไปจนถึงการเชื่อมต่อคอมพิวเตอร์ทั่วทั้งโลกที่เรียกว่าอินเทอร์เน็ต

1.5.8 **ราสเบอรี่ไพ** (Raspberry-Pi) [8] คือ คอมพิวเตอร์ขนาดเล็กที่สามารถเชื่อมต่อกับจอมอนิเตอร์ คีย์บอร์ด และเมาส์ได้ สามารถนำมาประยุกต์ใช้ในการทำการวิจัยทางด้านอิเล็กทรอนิกส์ การเขียนโปรแกรม หรือเป็นเครื่องคอมพิวเตอร์ตั้งโต๊ะขนาดเล็ก เป็นต้น

1.5.9 **เครื่องแม่ข่าย** (Server) [9] คือเครื่องคอมพิวเตอร์ หรือเครื่องแม่ข่ายที่ใช้สำหรับทำหน้าที่ให้บริการสิ่งต่าง ๆ กับคอมพิวเตอร์ หรือเครื่องลูกข่ายเครื่องอื่น ๆ เช่นเรื่องเกี่ยวกับการจัดการระบบใช้ไฟล์ข้อมูล และทรัพยากรต่าง ๆ ร่วมกันเป็นระบบเครือข่าย เป็นต้น

1.5.10 **ลงทะเบียนเพียงจุดเดียว** (Single Sign-On: SSO) [10] คือ การเข้าถึงการใช้บริการของระบบทั้งหมดได้ด้วยการพิสูจน์ตัวตนเพียงครั้งเดียว

1.5.11 **สน็อท** (Snort) [11] คือ ระบบตรวจจับและป้องกันการบุกรุกเครือข่ายแบบโอเพนซอร์สที่มีจุดเด่นของภาษาเป็นตัวกำหนดกฎเกณฑ์ โดยนำข้อดีของวิธีการตรวจสอบประเภทต่าง ๆ ที่ยึดตามซิกเนเจอร์ โพรโทคอล และความผิดปกติของเครือข่ายมารวมกันไว้

1.6 ระยะเวลาในการดำเนินงาน

ในการดำเนินงานจะแบ่งออกเป็น 3 ขั้นตอนหลัก คือ

1.6.1 ขั้นเตรียมการ

- ค้นคว้าข้อมูลเกี่ยวกับเรื่องที่สนใจ
- ค้นคว้าข้อมูลที่เกี่ยวข้องกับหัวข้อการวิจัย

- ศึกษาทำความเข้าใจข้อมูลที่เกี่ยวข้อง ได้แก่ ระบบพิสูจน์ตัวตน ระบบตรวจจับการบุกรุก เคอร์เบอรอส สน็อท ซีเคียวเชล (Secure Shell: SSH) และราสเบอรี่ไพ

1.6.2 ขั้นดำเนินการ

1.6.2.1 ออกแบบ

- ออกแบบระบบพิสูจน์ตัวตน
- ออกแบบระบบตรวจจับการบุกรุก

1.6.2.2 ลงมือปฏิบัติ

- ศึกษาวิเคราะห์ และติดตั้งระพิสูจน์ตัวตน
- ศึกษาวิเคราะห์ และติดตั้งระบบตรวจจับการบุกรุก

1.6.2.3 จัดทำคู่มือการใช้งาน

1.6.3 ขั้นสรุปและประเมินผล

1.6.3.1 ทดสอบ

- ทดสอบระบบ
- เปรียบเทียบประสิทธิภาพทางรูปแบบการโจมตี และเวลา

1.6.3.2 แก้ไขข้อผิดพลาด

และระยะเวลาในการดำเนินงานสามารถดูได้จากตารางสรุปการดำเนินงานดังนี้

1.7 ระยะเวลาในการดำเนินงาน

กิจกรรม/ขั้นตอนการดำเนินงาน	ระยะเวลาดำเนินงาน (ปีงบประมาณ 2561)											
	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
ขั้นเตรียมการ												
ศึกษาค้นคว้าข้อมูล	←	—	→									
ขั้นดำเนินการ												
ออกแบบการทำงาน			←	—	—	→						
เขียนโปรแกรมตามที่ออกแบบไว้					←	→						
เก็บผลการทดลอง						←	—	—	→			
พัฒนาโปรแกรมให้ดีขึ้น									←	→		
ขั้นสรุป และประเมินผล												
ประเมินผลการทดลอง										←	—	→