บทที่ 1

บทนำ

1.1 ความเป็นมาของปัญหา

ยูนิกซ์ (UNIX)เป็นระบบปฏิบัติการ (Operating System) ที่ถูกคิดค้นโดย เคน ทอมป์สัน (Ken Thompson) และ เดนนิส ริทชี (Dennis Ritchie) แห่งบริษัทเอที แอนด์ที (AT&T) หลังจากนั้นก็ได้มีผู้นำยูนิกซ์ไปติดตั้ง (port) ไปยังเครื่องคอมพิวเตอร์ต่างๆ ทำให้ยูนิกซ์เป็นที่รู้จักกันอย่างแพร่หลาย

เนื่องจากว่าผู้ออกแบบยูนิกซ์เป็นโปรแกรมเมอร์ จุดประสงค์ของยูนิกซ์ คือเพื่อให้โปรแกรมเมอร์ใช้ยูนิกซ์เป็นสภาพแวดล้อมในการพัฒนาโปรแกรม และเพื่อให้ใช้งานได้โดยสะดวก ดังนั้นผู้ออกแบบจึงไม่ได้คำนึงถึงระบบความมั่นคง (security) มากนัก (Ritchie, 1984) ต่อมาเทคโนโลยีทางด้านเครือข่าย(network) ได้เจริญก้าวหน้ามากขึ้น จึงได้มีผู้พัฒนาโปรแกรมเพื่อให้ระบบยูนิกซ์บนเครื่องต่างกัน สามารถติดต่อสื่อสารกันได้ ยังผลทำให้ผู้ใช้ที่อยู่บนเครื่องยูนิกซ์ต่างๆ สามารถใช้โปรแกรมสื่อสาร เช่น จดหมายอิเล็กทรอนิกส์ (Electronic Mail),ใช้เครื่องในระยะไกล (Remote Login) และ ส่งแฟ้มระหว่างเครื่อง (File Transfer) ซึ่งสิ่งเหล่านี้ทำให้การใช้งานยูนิกซ์แพร่หลายยิ่งขึ้น แต่ก็ทำให้การดูแลทางด้านความมั่นคงของระบบยูนิกซ์ซับซ้อนยิ่งขึ้นเช่นกัน

ในวันที่ 2 พฤศจิกายน พ.ศ. 2531 เครือข่ายอินเตอร์เนท (INTERNET) ซึ่งส่วนใหญ่ประกอบด้วย สถานีงาน (workstation) และคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการยูนิกซ์ถูกโปรแกรม เวอร์ม (Worm Program) ซึ่งเป็นโปรแกรมประเภทที่สามารถสร้างตัวเองใหม่ได้ (Self-Replicating program)เข้าบุกรุก ถึงแม้ว่าโปรแกรมเวอร์มจะไม่ได้ทำความเสียหายให้กับแฟ้มข้อมูลหรือขโมยข้อมูลใดๆก็ตาม แต่มันก็ได้เข้ารบกวนการทำงานของเครือ

ข่ายอินเตอร์เนท ทำให้ผู้ใช้ไม่สามารถใช้งานได้ตามปกติ (denial of service) ประมาณกันว่าทำให้เกิดความเสียหายมากกว่า 10 ล้านเหรียญสหรัฐ (Hayes, 1990)

เหตุการณ์ดังกล่าวทำให้เกิดความตื่นตัวทางด้าน การดูแลความมั่นคงของระบบยูนิกซ์มากขึ้น ทั้งนี้เนื่องจาก โปรแกรมเวอร์มได้อาศัยจุดหละหลวมในความมั่นคง (security hole) ของระบบยูนิกซ์ซึ่งได้รับการตีพิมพ์เผยแพร่เป็นที่ทราบกันทั่วไป แต่ว่าผู้จัดการระบบ (system administrator) ไม่ได้สนใจที่จะแก้ไข (Spafford, 1989)

ถึงแม้จะมีผู้กล่าวว่า ระบบยูนิกซ์มีระบบความมั่นคงน้อยกว่า ระบบปฏิบัติการแบบอื่น แต่ในทางปฏิบัติผู้จัดการระบบสามารถที่จะควบคุมระดับความมั่นคง ในระดับที่ตนเองต้องการได้ (Gramp, Morris, 1987)

ในปัจจุบัน ยูนิกซ์ได้ถูกนำไปติดตั้งในเครื่องคอมพิวเตอร์แทบทุกประเภท นับตั้งแต่เครื่องไมโครคอมพิวเตอร์ สถานีงาน (workstation) จนถึงซุปเปอร์คอมพิวเตอร์ และจากการที่ระบบเครือข่าย ได้ขยายขอบเขตกว้างขึ้น ทำให้ผู้ใช้คอมพิวเตอร์ธรรมดาต้องเข้ามายุ่งเกี่ยวกับความสลับซับซ้อน ของการดูแลระบบ (system administration) มากขึ้น ระบบยูนิกซ์ส่วนใหญ่จะมีโปรแกรมช่วยการดูแลระบบ ซึ่งทำให้ผู้จัดการระบบสามารถทำงานได้ง่ายขึ้น แต่ยังไม่มีโปรแกรม หรือ เครื่องมือที่จะช่วยตรวจสอบความมั่นคงให้กับผู้จัดการระบบ ผู้จัดการระบบจำเป็นที่จะต้องใช้ประสบการณ์ส่วนตัว ในการหาจุดหละหลวมในความมั่นคงของระบบของตน แต่เนื่องจากระบบยูนิกซ์เป็นระบบปฏิบัติการที่มีความสลับซับซ้อน ผู้จัดการระบบอาจมองข้ามบางจุด โดยเฉพาะผู้ที่ยังไม่มีประสบการณ์เพียงพอ (Brand, 1990)

โปรแกรมช่วยตรวจสอบความมั่นคงของระบบยูนิกซ์ จะช่วยแบ่งเบาภาระของผู้จัดการระบบ ทำให้ผู้จัดการระบบทราบถึงปัญหาที่เกิดขึ้น และสามารถแก้ไขหรือป้องกันปัญหาอันจะเกิดขึ้นได้

1.2 วัตถุประสงค์ของการวิจัย

เพื่อพัฒนาโปรแกรมช่วยตรวจสอบระบบความมั่นคงของ ระบบปฏิบัติการยูนิกซ์ตระกูลบีเอสดี 4.2 (4.2 BSD) และซิสเตมไฟว์ (System V)

1.3 ขอบเขตการวิจัย

1.3.1 โปรแกรมช่วยตรวจสอบระบบความมั่นคง สามารถที่จะนำมาใช้งานได้บนระบบปฏิบัติการยูนิกซ์ ตระกูลบีเอสดี 4.2 และซิสเตมไฟว์

1.3.2 โปรแกรมช่วยตรวจสอบระบบความมั่นคงจะแสดงข้อความให้ทราบถึงส่วนที่หละหลวมหรือจุดที่น่าสงสัย แต่จะไม่เข้าไปแก้ไขในส่วนนั้น ซึ่งโปรแกรมจะแนะนำวิธีแก้ไขให้และให้ผู้ใช้แก้ไขด้วยตนเอง

1.3.3 ภาษาที่ใช้ในการพัฒนา คือ ภาษาซี (C) , เบอร์นเชลล์ (Bourne shell),และโปรแกรมอรรถประโยชน์ (utility program) ต่างๆที่มีในระบบยูนิกซ์

1.3.4 ตัวเชื่อมโยงผู้ใช้ (user interface) ใช้โปรแกรมไลบรารี เคิร์ส (CURSES) ในการพัฒนา

1.4 ขั้นตอนการวิจัย

1.4.1 ศึกษาโครงสร้างระบบแฟ้มข้อมูลและไดเรคทอรีที่สำคัญของระบบยูนิกซ์

1.4.2 ศึกษาการใช้งานโปรแกรมไลบรารีเคิร์ส

1.4.3 ออกแบบตัวเชื่อมโยงผู้ใช้และมอดูลของโปรแกรมต่างๆ

1.4.4 พัฒนาโปรแกรม

1.4.5 ปรับแก้โปรแกรมเพื่อให้มีประสิทธิภาพเพิ่มขึ้น

1.4.6 สรุปผลการวิจัย และ ข้อเสนอแนะ

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 ทำให้ผู้ใช้ตระหนักถึงปัญหาของระบบความมั่นคงในเครื่องหรือเครือข่ายที่ตนเองรับผิดชอบ

1.5.2 ช่วยแบ่งเบาภาระของผู้ใช้ในการตรวจสอบระบบความมั่นคง

1.5.3 ทำให้ผู้ใช้สามารถทราบถึงจุดที่เกิดปัญหา และสามารถแก้ไขได้ทันท่วงที

1.5.4 สามารถใช้เป็นแนวทางในการพัฒนาระบบตรวจสอบความมั่นคงสำหรับยูนิกซ์รุ่น (version) ต่างๆที่เฉพาะเจาะจง