ความผิดพลาดของการรักษาความปลอดภัยในการทำงานของระบบคอมพิวเตอร์และสารสนเทศในองค์กร หมายถึงความเสียหายอย่างมากสำหรับองค์กร ดังนั้นจึงต้องมีการป้องกันความผิดพลาดที่อาจเกิดขึ้น รวมถึงการป้องกันการโจมตีจากผู้ไม่หวังดีต่อระบบ เพื่อลดความเสี่ยงต่อความเสียหายที่อาจเกิดขึ้น

จากปัญหาดังกล่าวเป็นแรงผลักดันให้มีแนวคิดและงานวิจัยในการป้องกันความเสียหายดังกล่าว โดยการเพิ่มความสามารถในด้านการรักษาความปลอดภัยให้กับระบบปฏิบัติการ เมื่อศึกษาจากระบบปฏิบัติการลินุกซ์ พบว่ามี 2 แนวทาง แนวทางหนึ่งคือ การเสริมความแข็งแกร่งให้กับระบบ ส่วนอีกแนวทางหนึ่งคือเปลี่ยนแปลงการควบคุมการเข้าถึงของระบบ ด้วยวิธีที่มีประสิทธิภาพสูงขึ้น เพื่อลดช่องทางในการโจมตีระบบ

ในงานวิจัยนี้ จึงได้ทำการวิเคราะห์ความสามารถในการป้องกันจุดอ่อนในรูปแบบต่างๆ โดยทำการคัดเลือกและจัดกลุ่มให้กับรายการของจุดอ่อนที่พบในระบบลินุกซ์ที่มีการรวบรวมในรายการซีวีอี และทำการวิเคราะห์การทำงานของการเสริมความปลอดภัยในระบบลินุกซ์ในการเพิ่มความแข็งแกร่ง และการใช้แอลเอสเอ็ม ซึ่งเป็นโครงร่างสำหรับการเพิ่มเติมการควบคุมการเข้าถึงของลินุกซ์ เพื่อทำการประเมินลักษณะของจุดอ่อนที่วิธีการเสริมความปลอดภัยในแต่ละแบบสามารถป้องกันได้ ซึ่งจากการวิจัย สามารถสรุปได้ว่า การเสริมความแข็งแกร่ง และการใช้แอลเอสเอ็ม มีความสามารถในการป้องกันจุดอ่อนในลักษณะที่ต่างกัน โดยการเสริมความแข็งแกร่ง สามารถป้องกันจุดอ่อนได้มากกว่า

Security flaws in computer and information systems in an organization mean a serious damage for the organization. The prevention of the system vulnerabilities and also the attack activities have to be concerned to reduced the risk of the damage.

From the stated reason, many researches and methods have been developed to prevent the system security vulnerability by extended the security parts in the operating system. In Linux system, there're 2 main methods: Hardening the operating system with suitable configuration, and extending the system access control with more effective methodology.

Consequently, this research is aimed to analyze and evaluate the vulnerability prevention ability of different protection methods. First, Linux known-vulnerability from CVE list have been selected and categorized. Then, the architecture and functionality of OS hardening and LSM which are selected protection methods have been analyzed. Then, the evaluation of the vulnerability characteristics that can be reduced by applying each method have been made. The research reveals that each method can prevent different vulnerability characteristic In overall, the OS hardening prevent more number of vulnerability than LSM.