การป้องกันบัฟเฟอร์โอเวอร์โฟลว์เป็นที่สนใจอย่างกว้างขวางในด้านความมั่นคงของคอมพิวเตอร์ จุดประสงค์ของการวิจัยนี้คือ นำเสนอวิธีการนำซีเคียวคานารีเวิร์ดมาทำให้เกิดผลวิธีใหม่ และประเมินผลในสองด้าน ได้แก่ ด้านการป้องกัน และด้านประสิทธิภาพ ซีเคียวคานารีเวิร์ดเป็นการแก้ปัญหาด้วยสถาปัตยกรรมที่มีพื้นฐานมาจากสองวิธีการที่มีอยู่แล้ว ได้แก่ ซีเคียวบิตและคานารีเวิร์ด เพื่อป้องกันการโจมตีด้วยบัฟเฟอร์โอเวอร์โฟลว์ในข้อมูลส่วนที่ไม่เป็นตัวควบคุมระบบ เช่น ตัวแปร และอาร์กิวเมนต์ เป็นต้น การทำให้เกิดผลนี้จัดทำบนซอฟต์แวร์เลียนแบบการทำงานของอุปกรณ์ฮาร์ดแวร์ชื่อ โบชส์ (BOCHS Emulator) ที่ดัดแปรแล้ว ซึ่งรันระบบปฏิบัติการลีนุกซ์ (เรดเฮด 6.2 เคอร์เนล 2.2.14) เมื่อประเมินผลแล้ว ผลลัพธ์แสดงให้เห็นว่า ซีเคียวคานารีเวิร์ดสามารถตรวจหาการโจมตีด้วยบัฟเฟอร์โอเวอร์โฟลว์ในข้อมูลส่วนที่ไม่เป็นตัวควบคุมระบบได้และยังครอบคลุมมากกว่าซีเคียวบิต นอกจากนี้ ประสิทธิภาพดีกว่างานเดิมอย่างเห็นได้ชัด การนำซีเคียวคานารีเวิร์ดมาทำให้เกิดผลด้วยวิธีการใหม่นี้ชี้ให้เห็นว่า ระบบมีความปลอดภัยมากขึ้น

235686

The possibility of buffer-overflow protection has generated wide interest in Computer Security. The purposes of this study are to propose a new method for implementing Secure Canary Word and to evaluate it in two aspects: protection and efficiency. Secure Canary Word is an architectursal approach based on two existing schemes, Secure Bit and Canary Word, for protecting against buffer-overflow attacks on non-control data (variables and arguments). The implementation was conducted in the modified BOCHS emulators running Linux (Red Hat 6.2 Kernel 2.2.14). When it is evaluated, the results showed that Secure Canary Word is not only able to detect buffer-overflow attacks on non-control data but it can also provide more coverage than that of Secure Bit. Furthermore, its efficiency is clearly better than that of the previous work. Our implementation suggests that system can be more secure with the new approach.