นายพัชร กกสูงเนิน : ผลของพารามิเตอร์ต่อความเร็วสำหรับการแฮชชิ่งของอาร์กอนสองไอ (EFFECT OF PARAMETERS ON HASHING SPEED OF ARGON2I)
อาจารย์ที่ปรึกษา : รองศาสตราจารย์ ดร.ศิรปัฐช์ บุญครอง, 88 หน้า.

การค้นคว้าอิสระนี้ ทำการทดลอง การแฮชชิ่งด้วย Argon2i เพื่อค้นหาว่าการปรับค่าพารามิเตอร์ ได้แก่ ความยาวของรหัสผ่าน ความยาวของ Salt ขนาดของ Memory size (k) Iteration number (t) Parallelism (p) และ Tag length (l) ขนาดใด ที่ใช้เวลาในการแฮชชิ่งที่น้อยที่สุดที่ Argon2i สามารถทำได้ เพื่อแก้ปัญหาของ Argon2i ที่มีจุดอ่อนด้านเวลาในการแฮชชิ่งที่ต้องใช้เวลานาน และ พารามิเตอร์ที่สามารถปรับแก้ไขได้หลากหลาย ทำให้หากเลือกปรับค่าได้ไม่เหมาะสมจะทำให้เวลาในการแฮชชิ่งนานเกินไปจนทำให้ผู้ใช้ระบบไม่พอใจ นอกจากนั้น ผู้วิจัยยังได้นำค่าพารามิเตอร์เหล่านี้มาทดลอง Avalanche Effect กับ แฮชชิ่งอัลกอริธึมอื่น ๆ ได้แก่ MD5 SHA1 และ SHA256 เพื่อเปรียบเทียบและประเมินด้านความปลอดภัยของ Argon2i ที่ได้เวลาที่น้อยที่สุด ว่ามีความปลอดภัยที่เพียงพอต่อการใช้งานจริง เมื่อเทียบกับ อัลกอริธึม ต่าง ๆ ที่ใช้งานจริงในปัจจุบัน สุดท้าย ผู้วิจัยได้ทดลองปรับเปลี่ยนพารามิเตอร์ของ Argon2i เป็นรายตัว เพื่อหาว่าการปรับขนาดของ พารามิเตอร์ตัวไหนที่มีผลต่อความปลอดภัยมากที่สุด

จากการวิจัย สามารถสรุปได้ว่า Argon2i สามารถทำให้ได้เวลาที่น้อยที่สุดโดยปรับค่าพารามิเตอร์ดังนี้ Memory size ปรับค่าเท่ากับ 4000 KiB และ Iteration number ปรับค่าเท่ากับ 2 และ Parallelism (p) ปรับค่าเท่ากับ 8 ซึ่งได้มาจากค่า 2 เท่าของ Threads CPU และ รหัสผ่าน ให้มีความยาวเท่ากับ 28 ตัวอักษร และ ค่า Salt ให้มีความยาวเท่ากับ 24 ตัวอักษร และ Tag length (l) ให้ปรับเป็นขนาด 32 bits ซึ่งเป็นค่าจะผลทดลองที่ได้เวลาที่ต่ำที่สุด และ ส่วนของการประเมินด้านความปลอดภัยเมื่อเทียบกับการปรับพารามิเตอร์ด้วยความยาวรหัสผ่าน จะมีผลต่อความปลอดภัยของ Argon2i มากที่สุดและเมื่อเทียบกับ อัลกอริธึมอื่น ๆ Argon2i ที่ปรับค่าพารามิเตอร์ให้ได้เวลาที่น้อยที่สุด นั้นมีความปลอดภัยที่เทียบเท่ากับ ได้แก่ MD5 SHA1 และ SHA256

สาขาวิชาเทคโนโลยีดิจิทัลและนิเทศศาสตร์ดิจิทัล ลายมือชื่อนักศึกษา _____
ปีการศึกษา 2566 ลายมือชื่ออาจารย์ที่ปรึกษา _____

PATCHARA KOKSUNGNOEN : EFFECT OF PARAMETERS ON HASHING SPEED OF ARGON2I: THESIS ADVISOR : ASSOC. PROF. SIRAPAT BOONKRONG, Ph.D. 88 PP.

ARGON2/ARGON2I/HASHINGPASSWORD/AVALANCHEEFFECT/ ARGON2IASSESSMENT

Experiment with hashing using Argon2i to determine how to adjust parameters such as password length, salt length, memory size (k), iteration number (t), parallelism (p), and tag length (l) will help optimise the security of the system. The objective of this independent study is to minimise the hashing time of Argon2i, addressing its weakness in prolonged hashing time and the presence of numerous adjustable parameters. Inappropriately adjusting these settings can result in excessively long hashing times, leading to user dissatisfaction. Additionally, these parameters were tested for the avalanche effect and compared with other hashing algorithms, including MD5, SHA1, and SHA256, to conduct a minimal-time security assessment of Argon2i, ensuring it is secure enough for practical use. By comparing Argon2i with various algorithms currently in use and experiment with each parameter, we can determine which ones have the greatest impact on safety.

The results indicate that the lowest time for Argon2i can be achieved by adjusting the following parameters: setting memory size to 4000 KiB, iteration number to 2, and parallelism to 8, derived from a value of 2 times the CPU threads. The password must be 28 characters long, the salt value should be 24 characters long, and the tag length should be adjusted to 32 bits, as this value yields the lowest time. Evaluate the security of Argon2i by examining the impact of password length on parameterisation. This aspect has the most significant effect on the safety of Argon2i.

School of Digital Technology and Communication Student's Signature_____

Academic Year 2023 Advisor's Signature_____