

การศึกษาปัจจัยที่มีอิทธิพลต่อการใช้งานได้และ ความปลอดภัยของรหัสผ่านแบบการ์ตูน The Study of Factors Influencing Usability and Security of Cartoon-based Passwords

วัชรินทร์ มธุรสพงศ์พันธ์ (Watcharin Mathurospongpan)* และ ณัฐรณันท์ หงส์วิทธิธร (Nuttanont Hongwarittorn)*

บทคัดย่อ

งานวิจัยนี้ ทำการทดลองเปรียบเทียบเพื่อหาปัจจัยที่มีอิทธิพลต่อประสิทธิภาพการใช้งานและความปลอดภัยของวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพแบบรูปตัวการ์ตูน โดยปัจจัยที่นำมาทดลองเปรียบเทียบ ได้แก่ ปัจจัยการใช้ตารางกริด ประกอบไปด้วย การมีตารางกริดกับไม่มีตารางกริด และปัจจัยรูปแบบการได้มาของรหัสผ่าน ประกอบไปด้วย การที่ผู้ใช้สร้างรหัสผ่านเองกับระบบสุ่มรหัสผ่านให้ ใช้รูปแบบการทดลอง 2x2 Between-Subjects Design กับผู้เข้าร่วมการทดลองทั้งหมด 60 คน แบ่งออกเป็น 4 กลุ่มด้วยวิธีการสุ่มกลุ่มละ 15 คน ได้แก่ กลุ่มที่มีตารางกริด ผู้ใช้สร้างรหัสผ่านเอง กลุ่มที่มีตารางกริด ระบบสุ่มรหัสผ่านให้ กลุ่มที่ไม่มีตารางกริด ผู้ใช้สร้างรหัสผ่านเอง และกลุ่มที่ไม่มีตารางกริด ระบบสุ่มรหัสผ่านให้ ประเมินผลด้วยประสิทธิภาพการใช้งานของรูปแบบการสร้างรหัสผ่านรูปภาพด้วย จำนวนครั้งที่ใช้เข้าระบบ เวลาเฉลี่ยที่ใช้เข้าระบบ และความสำเร็จในการเข้าระบบ และประเมินประสิทธิภาพความปลอดภัยด้วย จำนวนครั้งที่ใช้ในการโจรกรรมรหัสผ่าน เวลาเฉลี่ยที่ใช้ในการโจรกรรมรหัสผ่านและความสำเร็จในการโจรกรรมรหัสผ่าน และความพึงพอใจที่ผู้ใช้มีต่อระบบ ผลจากการทดลองชี้ให้เห็นว่า ปัจจัยที่ส่งผลต่อประสิทธิภาพการใช้งานและความปลอดภัยของวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพแบบรูปตัวการ์ตูนอย่างชัดเจนก็คือ การที่ผู้ใช้สร้างรหัสผ่านเองกับระบบสุ่มรหัสผ่านให้ โดยถ้าให้ผู้ใช้สร้างรหัสผ่านเองจะมีประสิทธิภาพการใช้งานที่ดีกว่า แต่ถาระบบสุ่มรหัสผ่านให้จะมีประสิทธิภาพความปลอดภัยที่ดีกว่า ส่วน

ของปัจจัยการมีตารางกริดส่งผลต่อประสิทธิภาพการใช้งานด้านเวลาเฉลี่ยในการเข้าระบบ 15 วันหลังจากสร้างรหัสผ่าน และส่งผลต่อประสิทธิภาพความปลอดภัยในด้านของเวลาเฉลี่ยในการโจรกรรมรหัสผ่าน โดยรหัสผ่านรูปภาพที่สร้างลงตารางกริดมีความปลอดภัยกว่ารหัสผ่านรูปภาพที่สร้างขึ้นแบบไม่มีตารางกริด

คำสำคัญ: รหัสผ่านรูปภาพ การ์ตูน ตารางกริด

Abstract

This research examined the two factors including the use of grid (grid and non-grid) and password generation (user-generated and system-generated) on usability and security. The 2x2 between-subjects design was employed to conduct the experiment with 60 participants. There were four experimental groups of 15 participants, which were grid and user-generated, grid and system-generated, non-grid and user-generated and non-grid and system-generated. All of participants were randomly assigned into each group. The usability was measured by the number of login, the average login time and the login success. The security was measured by the number of stolen, the average time spent by attacker to steal password and the success which passwords were stolen and also user satisfaction. The result indicated that password generation has an impact on usability and security of cartoon-based password. The passwords which were generated by users were

* คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์

more usable to the users. While the passwords which were generated by system were more secure. Moreover, the use of grid factor affected the average login time after passwords creation in 15 days. It also affected the average time spent by attacker to steal password. With respect to this finding, grid passwords should be more secure than non-grid passwords.

Keyword: Graphical password; Cartoon; Grid-based.

1. บทนำ

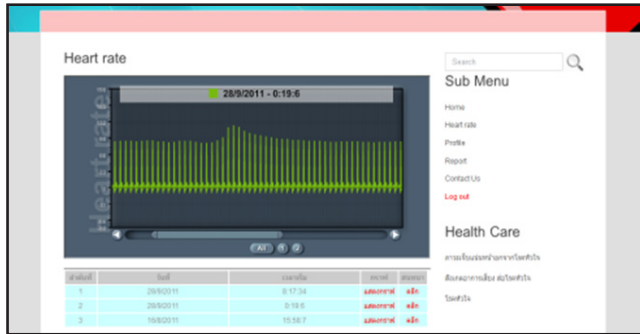
การพิสูจน์ตัวตน (Authentication) นั้นเป็นกระบวนการที่มีความสำคัญต่อระบบคอมพิวเตอร์เป็นอย่างมาก เนื่องจากว่าเป็นกระบวนการที่ใช้เพื่อคัดกรองว่าผู้ใช้ที่ต้องการเข้าสู่ระบบงานหรือข้อมูลนั้นมีสิทธิที่จะเข้าถึงระบบเหล่านี้จริงอย่างไรก็ตาม กลุ่มเซียนคอมพิวเตอร์ (Hacker) ได้มีความพยายามในการที่จะเข้าถึงระบบและข้อมูลเหล่านี้ด้วยการโจรกรรมรหัสผ่านของกระบวนการพิสูจน์ตัวตนด้วยวิธีการต่างๆ เช่น Brute force attack, Dictionary attack, Spyware, Shoulder surfing, และ Social engineering ดังนั้นการออกแบบวิธีการพิสูจน์ตัวตนที่มีประสิทธิภาพทั้งในเรื่องของ การใช้งาน (Usability) และมีความปลอดภัย (Security) จึงเป็นเรื่องที่สำคัญและน่าสนใจ ทำให้มีงานวิจัยที่เกี่ยวข้องกับกระบวนการพิสูจน์ตัวตนได้รับการพัฒนาอย่างต่อเนื่อง

วิธีการพิสูจน์ตัวตนด้วยการใช้ชื่อผู้ใช้งานและรหัสผ่านเป็นตัวอักษร นั้นเป็นวิธีการที่เป็นที่นิยมและใช้กันอย่างแพร่หลายตั้งแต่ในอดีตจนถึงปัจจุบัน ซึ่งปัญหาหลักของวิธีการนี้คือ การจดจำรหัสผ่าน จากการศึกษที่ผ่านมาแสดงให้เห็นว่าผู้ใช้จะเลือกตั้งรหัสผ่านที่สั้นและมีความหมายเพื่อที่จะจำได้ง่าย [1] ซึ่งส่งผลให้รหัสผ่านเหล่านี้สามารถถูกคาดเดาและถูกโจมตีได้ง่ายด้วยวิธีการ “small dictionary attack” [2], [3], [4] แต่ถ้ายึดรหัสผ่านที่ซับซ้อนคาดเดายาก ผู้ใช้ก็จะเกิดปัญหาในเรื่องของการลืมและระลึกถึงรหัสผ่าน จากการศึกษที่ผ่านมาแสดงให้เห็นว่ามนุษย์มีความสามารถในการจดจำรหัสผ่านได้จำกัด ทำให้ผู้ใช้ส่วนมากจะจดบันทึกรหัสผ่านไว้ [5] หรือใช้รหัสผ่านเดียวกันในทุกๆ บัญชี [6] ทำให้รหัสผ่านถูกโจรกรรมได้ง่ายและเกิดความไม่ปลอดภัยในทุกๆ บัญชีที่ใช้รหัสผ่านเดียวกันนี้

วิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ ได้ถูกคิดค้นขึ้นเพื่อเป็นทางเลือกในการแก้ไขปัญหาวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านตัวอักษร โดยมีงานวิจัยทางด้านจิตวิทยารองรับว่ามนุษย์สามารถจดจำและระลึกถึงรูปภาพได้ดีกว่าตัวอักษร [7], [8], [9] รหัสผ่านรูปภาพจึงถูกจดจำและระลึกถึงได้ง่ายกว่ารหัสผ่านตัวอักษร ในอดีตมีงานวิจัยทางด้านรหัสผ่านรูปภาพที่มีการประยุกต์วิธีการสร้างรหัสผ่านด้วยการสร้างรหัสผ่านบนตารางกริด ออกมามากมาย [10], [11], [12] ซึ่งวิธีการสร้างรหัสผ่านรูปภาพบนตารางกริดมีข้อดีก็คือสามารถเพิ่มความเป็นไปได้ของรหัสผ่านให้มากขึ้น ส่งผลให้ระบบมีความปลอดภัยสูงขึ้น อีกทั้งยังมีงานวิจัยทางด้านรหัสผ่านรูปภาพซึ่งมีการประยุกต์นำรูปตัวการ์ตูนมาใช้เป็นรหัสผ่าน [13] โดยมีแนวคิดที่ว่า มนุษย์จะมีตัวการ์ตูนที่ชอบตัวการ์ตูนในดวงใจ ซึ่งจะช่วยให้ระลึกถึงได้ง่ายกว่ารูปภาพชนิดอื่นๆ จากงานวิจัยที่ใช้รูปการ์ตูนเป็นรหัสผ่านรูปภาพแสดงให้เห็นว่า ผู้ใช้สามารถจดจำรูปภาพการ์ตูนได้ง่าย ดังนั้นงานวิจัยนี้จึงมีวัตถุประสงค์เพื่อศึกษาปัจจัยที่มีอิทธิพลต่อการใช้งานได้และความปลอดภัยของรหัสผ่านรูปภาพแบบตัวการ์ตูนโดยปัจจัยที่จะนำมาศึกษาเปรียบเทียบได้แก่ ปัจจัยการใช้ตารางกริด ประกอบไปด้วย การมีตารางกริดกับไม่มีตารางกริดและปัจจัยรูปแบบการได้มาของรหัสผ่าน ประกอบไปด้วย การที่ผู้ใช้สร้างรหัสผ่านเองกับระบบสุ่มรหัสผ่านให้ รายละเอียดของงานวิจัยในส่วนถัดไปจะกล่าวถึงงานวิจัยที่เกี่ยวข้อง ส่วนที่ 3 เป็นระเบียบวิธีวิจัย ส่วนที่ 4 เป็นผลการทดลอง ส่วนที่ 5 จะกล่าวถึง บทสรุป และส่วนสุดท้ายจะเป็นข้อเสนอแนะและงานวิจัยในอนาคต

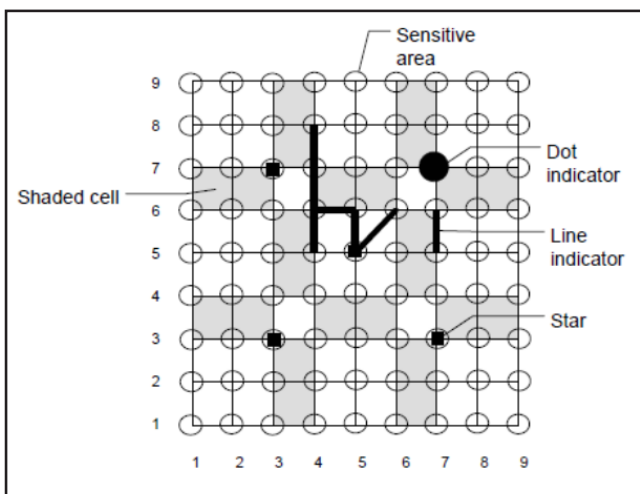
2. งานวิจัยที่เกี่ยวข้อง

ในปี 1999, Jermyn, Mayer, Monroe, Reiter, and Rubin [10] ได้เสนอวิธีการที่เรียกว่า “DAS (Draw-A-Secret)” ซึ่งผู้เข้าร่วมการทดลองจะต้องวาดรหัสผ่านของตนเองลงบนตารางกริดขนาด 5x5 ผู้ใช้สามารถวาดรหัสผ่านลงบนตารางกริดได้อย่างอิสระ จากงานวิจัยพบว่าความเป็นไปได้ของรหัสผ่านของวิธีนี้มีมากกว่าวิธีรหัสผ่านตัวอักษร แต่ปัญหาหลักของวิธีการนี้ก็คือ การวาดรหัสผ่านที่เป็นเส้น ซึ่งถ้าวาดเส้นใกล้กับตารางกริดหรือจุดตัดบนตาราง จะทำให้ระบบไม่สามารถแยกแยะได้ว่าเส้นที่วาดนั้นวาดลงบนตารางช่องใด



ภาพที่ 1 DAS (Draw-A-Secret) [10]

หลังจากนั้นในปี 2004, Thorpe and van Oorschot [11] ได้ศึกษางาน DAS เพิ่มเติม และได้เสนอวิธีที่เรียกว่า “Grid Selection” ซึ่งทำให้ผู้ใช้สามารถเลือกตารางกริดขนาด 5x5 จากขนาดตารางทั้งหมด 30x30 เพื่อนำมาใช้วาดรหัสผ่าน ทำให้มีความปลอดภัยมากขึ้น ต่อมาในปี 2006, Tao and Adams [12] ได้พัฒนาระบบที่เรียกว่า “Pass-Go” ซึ่งมีแนวคิดพื้นฐานอยู่บนวิธีการ “DAS” แต่จะต่างกันตรงที่ แทนที่จะวาดรหัสผ่านลงบนช่องกริด แต่จะให้อาตมาลงบนเส้นตารางหรือจุดตัดของช่องกริดแทน ทำให้ใช้งานง่ายกว่าและแก้ปัญหาการแยกแยะเส้นวาดว่าเป็นของตารางช่องใดได้อีกทั้งยังใช้ตารางกริดขนาดใหญ่กว่า ทำให้มีความปลอดภัยสูงกว่า จากตัวอย่างข้างต้นจะเห็นได้ว่า มีการศึกษาวิจัยที่มุ่งเน้นไปที่รหัสผ่านรูปภาพบนตารางกริดเนื่องจากว่ารหัสผ่านรูปภาพที่ออกแบบให้ใช้ตารางกริดนั้นมีข้อดีคือสามารถเพิ่มความเป็นไปได้ของรหัสผ่านทำให้ระบบมีความปลอดภัยมากขึ้น



ภาพที่ 2 Pass-Go [12]

ในปี 2007, Hinds and Ekwueme [13] ได้เสนอวิธีการที่เรียกว่า “ToonPasswords” ซึ่งผู้ใช้จะต้องสร้างรหัสผ่านด้วย

การเลือกรูปตัวการ์ตูน 1 รูปทั้งหมด 3 ครั้ง จากผลการศึกษาแสดงให้เห็นว่า 86% ของผู้ใช้สามารถจดจำและระลึกถึงรหัสผ่านได้หลังจากผ่านไป 30 วันนับจากวันที่สร้างรหัสผ่าน ซึ่งแสดงให้เห็นว่ารูปตัวการ์ตูนนั้นสามารถจดจำได้ง่าย

จากการศึกษางานวิจัยข้างต้นพบว่าที่ผ่านยังไม่มียานวิจัยใดทำการศึกษารหัสผ่านที่มีอิทธิพลต่อวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพแบบรูปตัวการ์ตูน ซึ่งเป็นเรื่องที่น่าสนใจ งานวิจัยนี้จึงทำการศึกษารหัสผ่านที่มีอิทธิพลต่อประสิทธิภาพการใช้งานและความปลอดภัยของวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพแบบรูปตัวการ์ตูน โดยปัจจัยที่นำมาทดลองเปรียบเทียบ ได้แก่ ปัจจัยการใช้ตารางกริด ประกอบไปด้วย การมีตารางกริดกับไม่มีตารางกริดและปัจจัยรูปแบบการได้มาของรหัสผ่าน ประกอบไปด้วย การที่ผู้ใช้สร้างรหัสผ่านเองกับระบบสุ่มรหัสผ่านให้ ซึ่งได้นำเอาข้อดีของรูปภาพตัวการ์ตูนเหมือนกับในงาน “ToonPasswords” และการสร้างรหัสผ่านบนตารางกริดมาประยุกต์ใช้ แต่จะมีวิธีการสร้างรหัสผ่านที่แตกต่างจากวิธีการของ “DAS” และ “PassGo” ประเมินผลด้วยประสิทธิภาพการใช้งาน ได้แก่ จำนวนครั้งที่ใช้เข้าระบบ เวลาเฉลี่ยที่ใช้เข้าระบบ และความสำเร็จในการเข้าระบบ และประสิทธิภาพความปลอดภัย ได้แก่ จำนวนครั้งที่ใช้ในการโจรกรรมรหัสผ่าน เวลาเฉลี่ยที่ใช้ในการโจรกรรมรหัสผ่าน และความสำเร็จในการโจรกรรมรหัสผ่าน และความพึงพอใจที่ผู้ใช้มีต่อระบบ

3. ระเบียบวิธีวิจัย

จากการศึกษาพบว่า ขนาดของตารางกริดนั้นสามารถมีได้หลายขนาด เพื่อที่จะทราบขนาดของตารางกริดที่เหมาะสมในการทดลอง ผู้วิจัยได้ทำการทดลองเบื้องต้น ด้วยการออกแบบวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพแบบรูปตัวการ์ตูนบนตารางกริดขนาดที่ต่างกัน ประกอบไปด้วยกริด 4 ขนาดได้แก่ 3x3 4x4 5x5 และ 5x3 และทำการทดลองเปรียบเทียบเพื่อหาขนาดของตาราง กริดที่ส่งผลต่อประสิทธิภาพการใช้งานที่ดีที่สุด ถึงแม้ว่าผลการทดลองจะออกมาว่าขนาดของตารางที่ใช้ในการทดลองส่งผลต่อประสิทธิภาพการใช้งานไม่แตกต่างกันอย่างมีนัยสำคัญ แต่จากการคำนวณหาความเป็นไปได้ของรหัสผ่านของแต่ละขนาดตารางพบว่าขนาดตาราง 4x4 มีความเหมาะสมที่สุดในการนำไปใช้

(วัชรินทร์ และ ณัฐชนนท์, 2012) ดังนั้นงานวิจัยนี้จึงได้เลือกใช้นาตาตารางกริด 4x4 ในการทำทดลอง

3.1 ตัวแปรและสมมติฐาน

ตัวแปรต้น งานวิจัยนี้ทำการศึกษาปัจจัยที่มีอิทธิพลต่อประสิทธิภาพการใช้งานและความปลอดภัยของวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพแบบรูปตัวการ์ตูน โดยปัจจัยที่นำมาทดลองเปรียบเทียบ ได้แก่ ปัจจัยการใช้ตารางกริดประกอบไปด้วย มีตารางกริด 4x4 กับไม่มีตารางกริด และปัจจัยรูปแบบการได้มาของรหัสผ่าน ประกอบไปด้วย การที่ผู้ใช้สร้างรหัสผ่านเองกับระบบสุ่มรหัสผ่านให้

ตัวแปรตาม งานวิจัยนี้วัดผลด้วยประสิทธิภาพการใช้งานและความปลอดภัยและความพึงพอใจของวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพแบบรูปตัวการ์ตูน ซึ่งรายละเอียดเป็นดังนี้

ประสิทธิภาพการใช้งาน

- 1) จำนวนครั้งที่ใช้หาระบบ
- 2) เวลาเฉลี่ยที่ใช้หาระบบ
- 3) ความสำเร็จในการหาระบบ

ประสิทธิภาพความปลอดภัย

- 1) จำนวนครั้งที่ใช้โจรกรรมรหัสผ่าน
- 2) เวลาเฉลี่ยที่ใช้โจรกรรมรหัสผ่าน
- 3) ความสำเร็จในการโจรกรรมรหัสผ่าน

ความพึงพอใจ

- 1) คะแนนความพึงพอใจจากแบบสอบถาม

สมมติฐาน คือ ปัจจัยการใช้ตารางกริด ประกอบไปด้วย มีตารางกริด 4x4 กับไม่มีตารางกริด และปัจจัยรูปแบบการได้มาของรหัสผ่าน ประกอบไปด้วย การที่ผู้ใช้สร้างรหัสผ่านเองกับระบบสุ่มรหัสผ่านให้ จะส่งผลต่อประสิทธิภาพการใช้งาน ประสิทธิภาพความปลอดภัย และความพึงพอใจที่ผู้ใช้มีต่อวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพแบบรูปตัวการ์ตูนแตกต่างกัน

3.2 การออกแบบการทดลอง

งานวิจัยนี้ใช้รูปแบบการทดลองเป็นแบบ 2x2 Between Subjects Design ซึ่งผู้เข้าร่วมการทดลองแต่ละคนจะได้รับมอบหมายให้ทำการทดลองคนละ 1 แบบ ใช้ผู้เข้าร่วมการทดลองทั้งหมด 60 คนแบ่งออกเป็นกลุ่มด้วยวิธีการสุ่มกลุ่มละ 15 คน ทั้งหมด 4 กลุ่มการทดลอง ได้แก่ กลุ่มที่มีตารางกริด ผู้ใช้สร้างรหัสผ่านเอง กลุ่มที่มีตารางกริด ระบบสุ่มรหัสผ่าน

ให้ กลุ่มที่ไม่มีตารางกริด ผู้ใช้สร้างรหัสผ่านเอง และกลุ่มที่ไม่มีตารางกริด ระบบสุ่มรหัสผ่านให้

3.3 ผู้เข้าร่วมการทดลอง

เนื่องจากงานวิจัยนี้มีข้อจำกัดในเรื่องของ ต้องมีการทำการทดลองซ้ำกับผู้เข้าร่วมการทดลอง จึงทำให้งานวิจัยนี้เลือกให้ผู้เข้าร่วมการทดลองที่เป็นพนักงานธนาคารกรุงเทพ ศูนย์คอมพิวเตอร์พระราม 3 ทั้งหมด 60 คน เป็นเพศชาย 36 คน เพศหญิง 24 คน ทั้งหมดมีประสบการณ์การใช้คอมพิวเตอร์มาอย่างน้อย 1 ปี มีอายุระหว่าง 21-45 ปี อายุเฉลี่ยประมาณ 30 ปี ผู้เข้าร่วมการทดลองทั้งหมดรู้จักและเคยผ่านการใช้งานกระบวนการพิสูจน์ตัวตนแบบรหัสผ่านตัวอักษรมาก่อน และมี 7 คนที่รู้จักและเคยผ่านการใช้งานรหัสผ่านรูปภาพ

3.4 เครื่องมือที่ใช้ในการทดลอง

โปรแกรมการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพแบบรูปตัวการ์ตูนที่ใช้ในงานวิจัยนี้ถูกพัฒนาด้วยภาษา PHP ทำงานบนระบบปฏิบัติการ Microsoft Windows XP Professional เรียกใช้ด้วยโปรแกรม Internet Explorer ในคอมพิวเตอร์แบบพกพา มีหน่วยประมวลผลที่อินเทล (Intel® Core™ 2 Duo) ความเร็วในการประมวลผล 2.0 กิกะเฮิร์ตซ์ มีหน่วยความจำหลัก 2 กิกะไบต์ และมีจอภาพแบบ LCD ขนาด 14 นิ้ว ที่มีความละเอียดของจอภาพอยู่ที่ 1366x768 พิกเซล ใช้โปรแกรม Camtasia Studio เพื่อบันทึกภาพขณะทำการทดลองและนำมาบันทึกผลการทดลองในภายหลัง และใช้แบบสอบถามเพื่อเก็บข้อมูลทั่วไปของผู้เข้าร่วมการทดลอง ก่อนทำการทดลอง และสุดท้ายใช้แบบประเมินเพื่อประเมินค่าความพึงพอใจหลังการทดลอง

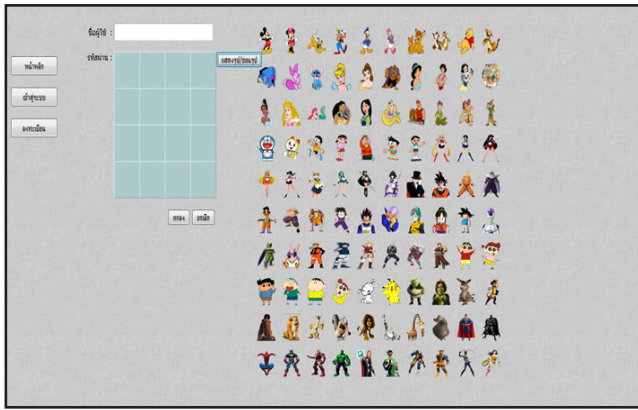
รูปตัวการ์ตูนที่นำมาใช้เป็นรหัสผ่านนั้นจะประกอบไปด้วย ตัวการ์ตูนจาก Walt Disney ตัวการ์ตูนจากการ์ตูนที่ฉายในโทรทัศน์ที่เป็นที่รู้จักดี และตัวการ์ตูนจากหนังสือการ์ตูนที่เป็นที่รู้จักดี รวมทั้งสิ้น 100 ตัว จัดเรียงเป็นแถวทั้งหมด 10 แถว แถวละ 10 รูป

3.5 การวัดผลการทดลอง

งานวิจัยนี้วัดผลด้วยประสิทธิภาพการใช้งาน ความปลอดภัยและความพึงพอใจของวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพแบบรูปตัวการ์ตูน ซึ่งรายละเอียดมีดังนี้

ประสิทธิภาพการใช้งาน

การวัดผลการทดลองด้านประสิทธิภาพการใช้งานนั้นจะ



ภาพที่ 3 ตัวอย่างหน้าจอเข้าสู่ระบบของโปรแกรมที่พัฒนาขึ้น

วัดจาก จำนวนครั้งที่ใช้เข้าระบบ เวลาเฉลี่ยที่ใช้เข้าระบบ และความสำเร็จในการเข้าระบบ

ประสิทธิภาพความปลอดภัย

การวัดผลการทดลองด้านประสิทธิภาพความปลอดภัยนั้นจะวัดจาก จำนวนครั้งที่ใช้โปรแกรมรหัสผ่าน เวลาเฉลี่ยที่ใช้โปรแกรมรหัสผ่าน และความสำเร็จในการโปรแกรมรหัสผ่าน

ความพึงพอใจ

วัดผลด้วยแบบสอบถามซึ่งมีจำนวน 12 ข้อ ซึ่งกำหนดวัดระดับความพึงพอใจออกเป็น 5 ระดับ คือ ระดับที่ 5 หมายถึง พึงพอใจมากที่สุด และระดับที่ 1 หมายถึง พึงพอใจน้อยที่สุด ทำการเก็บข้อมูลจากแบบสอบถามหลังจากที่ผู้เข้าร่วมการทดลองได้ทำการทดลองเสร็จ โดยจะเลือกตั้งคำถามที่สามารถชี้วัดได้ถึงประสิทธิภาพของปัจจัยที่นำมาใช้ในการทดลอง เช่น จำนวนรูป 100 รูป ความยาวรหัสผ่าน เป็นต้น อีกทั้งยังสามารถบ่งบอกได้ถึงประสิทธิภาพของตัวแปรต้นที่ใช้ในการทดลองว่ามีระดับความเหมาะสมมากน้อยเพียงใด โดยรายละเอียดคำถามเป็นดังตารางที่ 1

3.6 วิธีการทดลอง

การทดลองจะแบ่งออกเป็น การทดลองด้านการใช้งานและความปลอดภัย ในขั้นแรก ผู้วิจัยจะมอบแบบสอบถามให้ผู้เข้าร่วมการทดลองเพื่อเก็บข้อมูลทั่วไปก่อนผู้ทดลองจะเริ่มทำการทดลอง โดยที่ผู้วิจัยจะทำการอธิบายให้ผู้เข้าร่วมการทดลองฟังไปด้วยว่า ผู้วิจัยกำลังศึกษาวิจัยอะไร มีรายละเอียดแบบใด พร้อมกันนั้นผู้วิจัยจะเปิดโปรแกรมตัวทดสอบให้ผู้เข้าร่วมการทดลองได้ดูและลองใช้เบื้องต้นเพื่อที่จะให้ผู้เข้าร่วมการทดลองเกิดความคุ้นเคยและเข้าใจในสิ่งที่ตนเองได้รับมอบหมายให้ทำการทดลอง ในขั้นตอนนี้ผู้วิจัยจะอธิบายถึงการใช้งานของโปรแกรมและหน้าที่ของปุ่มต่างๆ

ตารางที่ 1 รายละเอียดแบบสอบถามความพึงพอใจ

ข้อที่	รายละเอียด	ระดับคะแนน				
		ระดับความพึงพอใจ				
		5	4	3	2	1
1	รูปภาพตัวการ์ตูนมีความชัดเจน					
2	ขนาดรูปภาพตัวการ์ตูนมีความเหมาะสม					
3	รูปภาพตัวการ์ตูนมีให้เลือก 100 รูป มีความเหมาะสม					
4	รูปภาพตัวการ์ตูนที่ใช้ทั้งหมดมีความเป็นที่รู้จักอย่างดี					
5	รหัสผ่านยาว 6 รูป มีความเหมาะสม					
*6	การที่ มี/ไม่มี การใช้ตารางในการสร้างรหัสผ่านรูปภาพมีความเหมาะสม					
*7	การสร้างรหัสผ่านรูปภาพด้วยการสร้างรหัสผ่านด้วยตนเอง/ระบบสุ่มรหัสผ่านให้ มีความเหมาะสม					
8	ตำแหน่งการจัดวางของตารางและรูปภาพตัวการ์ตูนมีความเหมาะสม					
9	รูปแบบรหัสผ่านสามารถจดจำได้ง่าย					
10	ระบบมีความปลอดภัย					
11	โปรแกรมสามารถใช้งานได้ง่าย					
12	ความเหมาะสมของระบบในการนำไปใช้เป็นรูปแบบรหัสผ่านจริง					

*คำถามจะแตกต่างกันไปตามแต่ละกลุ่มทดลอง

และอธิบายให้ผู้เข้าร่วมการทดลองต้องทำการทดลองอย่างไรตามขั้นตอน เมื่อผู้เข้าร่วมการทดลองพร้อม จึงเริ่มทำการทดลอง โดยจะให้ผู้เข้าร่วมการทดลองทำการสุ่มจับคู่เพื่อเตรียมการทดลองในด้านความปลอดภัย โดยผู้วิจัยจะเปิดโปรแกรมตัวทดลองจริงขึ้นมา และทำการเปิดโปรแกรม Camtasia Studio เพื่อบันทึกภาพการทดลอง โดยการทดลองจะเริ่มจากโปรแกรมจะเริ่มอยู่ที่หน้าหลัก หลังจากนั้นให้ผู้เข้าร่วมการทดลองทำการคลิกที่ปุ่ม “ลงทะเบียน” เพื่อเข้าสู่หน้าลงทะเบียนเพื่อสร้างชื่อผู้ใช้งานและรหัสผ่านสำหรับเข้าสู่ระบบ ซึ่งชื่อผู้ใช้งานทางผู้วิจัยจะเป็นคนกำหนดให้ ดังนั้นผู้เข้าร่วมการทดลองจึงมีหน้าที่สร้างรหัสผ่านเท่านั้น โดยวิธีการสร้างรหัสผ่านของโปรแกรมนั้นจะแตกต่างกันไปตามแต่ละปัจจัยการทดลองซึ่งมีรายละเอียดดังนี้

- ในกรณีที่ผู้ใช้สร้างรหัสผ่านเอง ผู้เข้าร่วมการทดลองจะ

ต้องสร้างรหัสผ่านด้วยการเลือกรูปตัวการ์ตูน 6 รูปจากทั้งหมด 100 รูป ไปจัดเรียงลงในตารางกริดขนาด 4x4 สามารถจัดเรียงได้อย่างอิสระ (6 รูป 6 ตำแหน่ง) สำหรับกลุ่มการทดลองแบบมีตารางกริด ส่วนกลุ่มการทดลองแบบไม่มีตารางกริด ให้จัดเรียงกันจากซ้ายไปขวา เหมือนกับการสร้างรหัสผ่านตัวอักษร ตัวการ์ตูนที่เลือกใช้สามารถเลือกใช้ซ้ำได้

- ในกรณีระบบสุ่มรหัสผ่านให้ ผู้เข้าร่วมการทดลองจะต้องกดที่ปุ่ม “สุ่มรหัสผ่าน” เพื่อที่จะให้ระบบทำการสุ่มรหัสผ่านให้ โดยให้กดเพียงครั้งเดียวและให้ใช้รหัสผ่านที่ระบบสุ่มให้ได้เลย

หลังจากผู้เข้าร่วมการทดลองสร้างรหัสผ่านเสร็จก็ให้กดปุ่ม “ยืนยันการลงทะเบียน” หลังจากนั้นผู้เข้าร่วมการทดลองจะต้องทำการเข้าสู่ระบบทันที 1 รอบ โดยให้กดที่ปุ่ม “เข้าสู่ระบบ” เพื่อเข้าสู่หน้าระบบ ซึ่งในขั้นตอนนี้จะให้คู่ของผู้เข้าร่วมการทดลองทำการยืนดูอยู่ด้วย หลังจากนั้นผู้เข้าร่วมการทดลองจะต้องทำการกรอกชื่อผู้ใช้ที่ผู้วิจัยกำหนดให้ และกรอกรหัสผ่านที่ได้สร้างไว้ในขั้นตอนลงทะเบียนให้ถูกต้อง เพื่อที่จะเข้าสู่ระบบได้สำเร็จ โดยการกรอกรหัสผ่านไม่จำเป็นต้องกรอกตามลำดับก่อน-หลัง เพียงแค่กรอกให้รูปตัวการ์ตูนถูกต้องและถูกตำแหน่งก็พอ เมื่อผู้เข้าร่วมการทดลองกรอกชื่อผู้ใช้และรหัสผ่านเสร็จก็ให้คลิกที่ปุ่ม “ตกลง” เพื่อเข้าสู่ระบบ ผู้เข้าร่วมการทดลองสามารถกรอกรหัสผ่านผิดได้ทั้งหมด 5 ครั้งต่อการพยายามเข้าสู่ระบบ 1 รอบ เมื่อกรอกผิดครบ 5 ครั้งจะถือว่าเข้าระบบล้มเหลว การทดลองจะเสร็จสิ้นก็ต่อเมื่อผู้เข้าร่วมการทดลองเข้าสู่ระบบสำเร็จ 1 ครั้งหรือล้มเหลวครบ 5 ครั้ง หลังจากการทดลองผู้วิจัยจะขอให้ผู้เข้าร่วมการทดลองทำการตอบแบบสอบถามเพื่อที่จะวัดความพึงพอใจของผู้เข้าร่วมการทดลองที่มีต่อโปรแกรมการพิสูจน์ตัวตนที่ผู้วิจัยได้ออกแบบ และหลังจากผ่านไป 3 วัน และ 15 วัน ผู้วิจัยจะให้ผู้เข้าร่วมการทดลองทุกกลุ่มทำการทดลองซ้ำอีกครั้งตามลำดับ โดยจะให้ผู้เข้าร่วมการทดลองทำการพยายามเข้าสู่ระบบ 1 รอบ ซึ่งรายละเอียดการทดลองครั้งนี้จะเหมือนกันกับการทดลองการเข้าสู่ระบบในครั้งแรก

ในส่วนของการทดลองด้านความปลอดภัย จะให้คู่ของผู้เข้าร่วมการทดลองที่ผ่านการยินยอมดูของตนเองขณะที่ทำการเข้าระบบ ทำการเข้าระบบด้วยชื่อผู้ใช้และรหัสผ่านของตัวเองของตนเอง ซึ่งจะทำให้การทดลองทั้งหมด 1 รอบ ภายใน

วันแรกที่สร้างชื่อผู้ใช้งานและรหัสผ่านเสร็จ โดยมีเงื่อนไขเหมือนเดิมคือ สามารถใส่ชื่อผู้ใช้และรหัสผ่านผิดได้ไม่เกิน 5 ครั้ง ถ้าใส่ผิดครบ 5 ครั้ง จะถือว่าเข้าสู่ระบบล้มเหลว โดยตั้งแต่ต้นจนจบกระบวนการการทดลอง ผู้วิจัยได้เฝ้าสังเกตการณ์อยู่ตลอดเวลา

4. ผลการทดลอง

หลังจากทำการทดลองเสร็จสิ้นจะนำผลที่ได้จากการทำการทดลอง ได้แก่ ผลการทดลองทางด้านประสิทธิภาพการใช้งาน ประกอบไปด้วย จำนวนครั้งที่ใช้เข้าระบบ เวลาเฉลี่ยที่ใช้เข้าระบบ และความสำเร็จในการเข้าระบบ ผลการทดลองทางด้านประสิทธิภาพความปลอดภัย ประกอบไปด้วย จำนวนครั้งที่ใช้ในการโจรกรรมรหัสผ่าน เวลาเฉลี่ยที่ใช้ในการโจรกรรมรหัสผ่าน และความสำเร็จในการโจรกรรมรหัสผ่าน และผลคะแนนความพึงพอใจที่ผู้ใช้มีต่อระบบ ไปวิเคราะห์หาความแตกต่าง ซึ่งได้ผลดังนี้

4.1 การวิเคราะห์ผลการทดลอง

1. ประสิทธิภาพการใช้งาน

ผลการทดลองจะมีทั้งหมด 3 ชุด ได้แก่ ผลการทดลองของวันแรกที่สร้างรหัสผ่าน ผลการทดลองของ 3 วันหลังจากสร้างรหัสผ่าน และผลการทดลองของ 15 วันหลังจากสร้างรหัสผ่าน ซึ่งจะนำไปวิเคราะห์ด้วยวิธีการ Independent-Sample T test สำหรับจำนวนครั้งและเวลา และวิธีการ Mann-Whitney U สำหรับความสำเร็จในการเข้าสู่ระบบ โดยสามารถสรุปผลการวิเคราะห์ได้ดังตารางที่ 2

จากตารางที่ 2 แสดงให้เห็นว่า ปัจจัยที่ส่งผลกระทบต่อประสิทธิภาพการใช้งานของวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพแบบรูปตัวการ์ตูนให้มีความแตกต่างกันอย่างมีนัยสำคัญ คือ ปัจจัยการที่ผู้ใช้สร้างรหัสผ่านเองกับระบบสุ่มรหัสผ่านให้โดยถ้าให้ผู้ใช้สร้างรหัสผ่านเองจะส่งผลให้มีประสิทธิภาพการใช้งานที่ดีกว่าทั้งในเรื่องของ มีจำนวนครั้งที่ใช้เข้าระบบน้อยกว่า มีเวลาเฉลี่ยที่ใช้เข้าระบบน้อยกว่า และมีความสำเร็จในการเข้าระบบมากกว่า

ในส่วนของปัจจัยการมีตารางกริดพบว่าส่งผลกระทบต่อประสิทธิภาพการใช้งานด้านเวลาเฉลี่ยที่ใช้เข้าระบบ 15 วัน หลังจากสร้างรหัสผ่าน โดยรหัสผ่านรูปภาพที่สร้างแบบไม่มีตารางกริดจะมีเวลาเฉลี่ยที่ใช้เข้าระบบน้อยกว่าแบบมีตารางกริด



ตารางที่ 2 สรุปผลการวิเคราะห์ผลการทดลองทางด้านประสิทธิภาพการใช้งาน

ปัจจัยที่ศึกษา	ค่าเฉลี่ยของผลการทดลองทางด้านประสิทธิภาพการใช้งาน								
	จำนวนครั้งที่ใช้ซ้ำระบบ (ครั้ง)			เวลาเฉลี่ยที่ใช้ซ้ำระบบ (วินาที)			ความสำเร็จในการเข้าระบบ (%)		
	วันแรก	3 วัน	15 วัน	วันแรก	3 วัน	15 วัน	วันแรก	3 วัน	15 วัน
มีตารางกริด 4x4	1.73	2.40	2.77	32.34	38.28	35.06	86.67	73.33	63.33
ไม่มีตารางกริด	1.30	2.60	2.70	27.89	31.29	27.31	93.33	73.33	66.67
P-Value	0.174	0.664	0.891	0.278	0.176	0.050	0.393	1.000	0.788
ผู้ใช้สร้างรหัสผ่านเอง	1.03	1.20	1.17	18.15	20.62	21.33	100.00	100.00	100.00
ระบบสุ่มรหัสผ่านให้	2.00	3.80	4.30	42.09	48.95	41.04	80.00	46.67	30.00
P-Value	0.003	0.000	0.000	0.000	0.000	0.000	0.010	0.000	0.000

แตกต่างกันอย่างมีนัยสำคัญที่ระดับความเชื่อมั่น 95%

ตารางที่ 3 สรุปผลการวิเคราะห์ผลการทดลองทางด้านประสิทธิภาพความปลอดภัยในเรื่องของ จำนวนครั้งและเวลาเฉลี่ยที่ใช้โจรกรรมรหัสผ่าน

กลุ่มทดลอง	ค่าเฉลี่ยของผลการทดลองทางด้านประสิทธิภาพความปลอดภัย	
	ความปลอดภัย	
	จำนวนครั้งที่ใช้โจรกรรมรหัสผ่าน(ครั้ง)	เวลาเฉลี่ยที่ใช้โจรกรรมรหัสผ่าน (วินาที)
มีตารางกริด 4x4 ผู้ใช้สร้างรหัสผ่านเอง	1.07	18.93
มีตารางกริด 4x4 ระบบสุ่มรหัสผ่านให้	4.73	36.65
ไม่มีตาราง กริด ผู้ใช้สร้างรหัสผ่านเอง	1.13	16.43
ไม่มีตาราง กริด ระบบสุ่มรหัสผ่านให้	4.85	26.45
P-Value Factor A	0.534	0.000
P-Value Factor B	0.000	0.000
P-Value Factor A*B	0.861	0.032

แตกต่างกันอย่างมีนัยสำคัญที่ระดับความเชื่อมั่น 95%

Factor A = การใช้ตารางกริด

Factor B = รูปแบบการได้มาของรหัสผ่าน

2. ประสิทธิภาพความปลอดภัย

ผลการทดลองจะมี 1 ชุด ซึ่งจะทำให้การทดลองภายในวันแรกที่สร้างรหัสผ่าน ซึ่งจะนำไปวิเคราะห์ด้วยวิธีการ Two-way ANOVA สำหรับจำนวนครั้งและเวลา และวิธีการ Mann-Whitney U สำหรับความสำเร็จในการโจรกรรม โดยสามารถ

สรุปผลการวิเคราะห์ได้ดังตารางที่ 3 และ 4

ตารางที่ 4 สรุปผลวิเคราะห์ผลการทดลองทางด้านประสิทธิภาพความปลอดภัยในเรื่องของ ความสำเร็จในการโจรกรรมรหัสผ่าน

ปัจจัยที่ศึกษา	ค่าเฉลี่ยของผลการทดลองทางด้านประสิทธิภาพความปลอดภัย
	ความสำเร็จในการโจรกรรมรหัสผ่าน (%)
มีตารางกริด 4x4	57.69
ไม่มีตารางกริด	57.14
P-Value	0.968
ผู้ใช้สร้างรหัสผ่านเอง	100.00
ระบบสุ่มรหัสผ่านให้	4.17
P-Value	0.000

แตกต่างกันอย่างมีนัยสำคัญที่ระดับความเชื่อมั่น 95%

จากตารางที่ 3 และ 4 แสดงให้เห็นว่า ปัจจัยที่ส่งผลต่อประสิทธิภาพความปลอดภัยของวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพแบบรูปตัวการคูณให้มีความแตกต่างกันอย่างมีนัยสำคัญ คือ ปัจจัยการที่ผู้ใช้สร้างรหัสผ่านเองกับระบบสุ่มรหัสผ่านให้โดยถ้าให้ระบบสุ่มรหัสผ่านให้จะส่งผลให้มีประสิทธิภาพการใช้งานที่ดีกว่าทั้งในเรื่องของ มีจำนวนครั้งที่ใช้โจรกรรมรหัสผ่านมากกว่า มีเวลาเฉลี่ยที่ใช้โจรกรรมรหัสผ่านมากกว่า และมีความสำเร็จในการโจรกรรมรหัสผ่านน้อยกว่า

ในส่วนของปัจจัยการมีตารางกริดพบว่าส่งผลต่อประสิทธิภาพความปลอดภัยด้านเวลาเฉลี่ยที่ใช้โจรกรรมรหัสผ่านโดยรหัสผ่านรูปภาพที่สร้างลงบนตารางกริดจะมีเวลาเฉลี่ยที่ใช้โจรกรรมรหัสผ่านมากกว่าแบบไม่มีตารางกริด

จากตารางที่ 3 ยังแสดงให้เห็นอีกว่า อิทธิพลร่วมระหว่างปัจจัยการใช้ตารางกริดและรูปแบบการได้มาของรหัสผ่านพบว่า ส่งผลต่อเวลาเฉลี่ยที่ใช้โจรกรรมรหัสผ่าน โดยถ้าสร้างรหัสผ่านแบบมีตารางกริดและระบบสุ่มรหัสผ่านให้จะใช้เวลาเฉลี่ยที่ใช้โจรกรรมรหัสผ่านมากกว่าแบบไม่มีตารางกริดและผู้ใช้สร้างรหัสผ่านเอง

นอกจากนี้ผู้วิจัยยังได้ทำการคำนวณความเป็นได้ทั้งหมดของรหัสผ่านของระบบที่ออกแบบ โดยสามารถคำนวณได้ดังนี้



ความเป็นไปได้ของรหัสผ่านทั้งหมดของแบบมีตารางกริดคือ

$$C_{S,N} \times K^N \quad (1)$$

ความเป็นไปได้ของรหัสผ่านทั้งหมดของแบบไม่มีตารางกริดคือ

$$K^N \quad (2)$$

โดย

S คือ ขนาดของตารางทั้งหมด

N คือ จำนวนรูปตัวการคูณที่ใช้ตั้งรหัสผ่าน

K คือ จำนวนรูปตัวการคูณที่มีให้เลือกทั้งหมด

ดังนั้นความเป็นไปได้ของรหัสผ่านทั้งหมดของระบบที่ออกแบบจึงคำนวณได้ดังนี้

แบบมีตารางกริด 4x4

$$C_{16,6} \times 100^6 = 8.008 \times 10^{15}$$

แบบไม่มีตารางกริด

$$100^6 = 10^{12} \quad (3)$$

3. ความพึงพอใจที่ผู้ใช้มีต่อระบบ

หลังจากทำการทดลองเสร็จ ผู้วิจัยจะให้ผู้เข้าร่วมการทดลองตอบแบบสอบถามทางด้านความพึงพอใจที่มีต่อระบบ และทำการรวบรวมคะแนนความพึงพอใจไปวิเคราะห์หาความแตกต่างด้วยวิธีการ Two-way ANOVA โดยสามารถสรุปผลการวิเคราะห์ได้ดังตารางที่ 5

จากตารางที่ 5 แสดงให้เห็นว่า ปัจจัยที่ส่งผลต่อคะแนนความพึงพอใจที่ผู้ใช้มีต่อระบบวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพแบบรูปตัวการคูณให้มีความแตกต่างกันอย่างมีนัยสำคัญ คือ ปัจจัยการที่ผู้ใช้สร้างรหัสผ่านเองกับระบบสุ่มรหัสผ่านให้ โดยถ้าให้ผู้ใช้สร้างรหัสผ่านเองจะมีคะแนนความพึงพอใจมากกว่าแบบระบบสุ่มรหัสผ่านให้โดยกลุ่มที่มีคะแนนความพึงพอใจมากที่สุดก็คือ กลุ่มไม่มีตารางกริด ผู้ใช้สร้างรหัสเอง โดยมีระดับคะแนนความพึงพอใจอยู่ที่ระดับพึงพอใจมาก

5. อภิปรายและสรุปผลการทดลอง

งานวิจัยนี้ได้ทำการศึกษาถึงปัจจัยที่ส่งผลกระทบต่อประสิทธิภาพการใช้งาน ความปลอดภัยและคะแนนความพึงพอใจที่ผู้ใช้มีต่อวิธีการพิสูจน์ตัวตนแบบรหัสผ่านรูปภาพแบบรูปตัวการคูณ ซึ่งปัจจัยที่ทำการศึกษาได้แก่ ปัจจัยการใช้ตารางกริด ประกอบไปด้วย การมีตารางกริดกับไม่มีตาราง

ตารางที่ 5 สรุปผลวิเคราะห์ผลการทดลองทางด้านความพึงพอใจที่ผู้ใช้มีต่อระบบ

กลุ่มทดลอง	ค่าเฉลี่ยของผลการทดลองทางด้านความพึงพอใจที่ผู้ใช้มีต่อระบบ
	คะแนนความพึงพอใจที่ผู้ใช้มีต่อระบบ
มีตารางกริด 4x4 ผู้ใช้สร้างรหัสผ่านเอง	3.82
มีตารางกริด 4x4 ระบบสุ่มรหัสผ่านให้	3.58
ไม่มีตารางกริด ผู้ใช้สร้างรหัสผ่านเอง	4.09
ไม่มีตารางกริด ระบบสุ่มรหัสผ่านให้	3.46
P-Value Factor A	0.669
P-Value Factor B	0.012
P-Value Factor A*B	0.251

แตกต่างกันอย่างมีนัยสำคัญที่ระดับความเชื่อมั่น 95%

Factor A = การใช้ตารางกริด

Factor B = รูปแบบการได้มาของรหัสผ่าน

กริด และปัจจัยรูปแบบการได้มาของรหัสผ่าน ประกอบไปด้วย การที่ผู้ใช้สร้างรหัสผ่านเองกับระบบสุ่มรหัสผ่านให้ โดยจากผลการทดลองสามารถสรุปได้ว่า ปัจจัยที่ส่งผลต่อประสิทธิภาพการใช้งานและความปลอดภัยของวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพแบบรูปตัวการคูณอย่างชัดเจนก็คือ การที่ผู้ใช้สร้างรหัสผ่านเองกับระบบสุ่มรหัสผ่านให้ โดยถ้าให้ผู้ใช้สร้างรหัสผ่านเองจะมีประสิทธิภาพการใช้งานที่ดีกว่า แต่ถ้าระบบสุ่มรหัสผ่านให้จะมีประสิทธิภาพความปลอดภัยที่ดีกว่า ส่วนของปัจจัยการมีตารางกริดส่งผลต่อประสิทธิภาพการใช้งานด้านเวลาเฉลี่ยในการเข้าระบบ 15 วันหลังจากสร้างรหัสผ่าน และส่งผลต่อประสิทธิภาพความปลอดภัยในด้านของเวลาเฉลี่ยในการโจรกรรมรหัสผ่าน โดยรหัสผ่านรูปภาพที่สร้างลงตารางกริดมีความปลอดภัยกว่ารหัสผ่านรูปภาพที่สร้างขึ้นแบบไม่มีตารางกริด

ในส่วนของ อิทธิพลร่วมระหว่างปัจจัยการใช้ตารางกริดและรูปแบบการได้มาของรหัสผ่าน พบว่า ส่งผลต่อเวลาเฉลี่ยที่ใช้โจรกรรมรหัสผ่าน โดยถ้าสร้างรหัสผ่านแบบมีตารางกริดและระบบสุ่มรหัสผ่านให้จะใช้เวลาเฉลี่ยที่ใช้โจรกรรมรหัสผ่านมากกว่าแบบไม่มีตารางกริดและผู้ใช้สร้างรหัสผ่านเอง

จากการที่งานวิจัยนี้เป็นงาน ToonPasswords [13] มาประยุกต์ โดยมีจุดที่แตกต่างกันก็คือ มีการนำตารางกริด

และวิธีการสร้างรหัสผ่านแบบระบบสุ่มรหัสผ่านให้มาประยุกต์ใช้ซึ่งถือเป็นจุดเด่นของงานวิจัยนี้ เนื่องจากว่าการศึกษาค้นคว้ายังไม่มียานวิจัยใดที่ทำการทดลองสร้างรหัสผ่านรูปภาพแบบให้ระบบสุ่มรหัสผ่านให้อีกทั้งการนำตารางกริดมาประยุกต์ใช้ก็มีผลให้งานวิจัยนี้มีประสิทธิภาพความปลอดภัยที่สูงกว่า อีกทั้งการใช้จำนวนรูปตัวการ์ตูนที่มากกว่าก็ช่วยเพิ่มความยากในการคาดเดารหัสผ่านให้มากขึ้น เนื่องจากว่ามีความเป็นไปได้ของรหัสผ่าน (password space) ที่มากกว่านั่นเอง ($8.008 \times 10^{15} > 40^3$)

ผู้เข้าร่วมการทดลองต่างมีความคิดเห็นไปในแนวทางเดียวกันว่า วิธีการสร้างรหัสผ่านแบบให้ระบบสุ่มรหัสผ่านให้ นั้นไม่เหมาะสมที่จะนำไปใช้งาน เนื่องจากว่าทำให้เกิดปัญหาในการจดจำและระลึกถึงรหัสผ่าน ถึงแม้ว่าจะช่วยให้ระบบมีความปลอดภัยสูงขึ้น ซึ่งสอดคล้องกับปัญหาของรหัสผ่านตัวอักษร อย่างไรก็ตาม งานวิจัยนี้มีข้อได้เปรียบกว่ารหัสผ่านตัวอักษร ไม่ว่าจะเป็น ในแง่ปัจจัยทางจิตวิทยาที่รองรับว่ามนุษย์สามารถจดจำและระลึกถึงรูปภาพได้ดีกว่าตัวอักษร [7], [8], [9] ซึ่งสามารถนำไปประยุกต์ใช้ได้กว้างกว่าเช่น นำไปใช้กับผู้ใช้ที่ไม่รู้ภาษาอังกฤษ อย่างไรก็ตามรหัสผ่านตัวอักษรก็ยังมีจุดเด่นในเรื่องของเป็นที่รู้จักมานานและคนส่วนมากจะมีความเคยชินกับระบบ

6. ข้อเสนอแนะและงานวิจัยในอนาคต

1) ทำการทดลองทางด้านประสิทธิภาพการใช้งานหลังจากเวลาผ่านไปนับจากวันแรกที่สร้างรหัสผ่านนานกว่านี้ เช่น 30 วัน 45 วัน เป็นต้น เพื่อเพิ่มความแม่นยำในส่วนของปัจจัยการมีตารางกริด 4x4 กับไม่มีตารางกริด เนื่องจากว่าผลการทดลองของ 15 วันหลังจากสร้างรหัสผ่านที่ได้ในงานวิจัยนี้นั้น แสดงให้เห็นว่า ปัจจัยการมีตารางกริด 4x4 กับไม่มีตารางกริด เริ่มที่จะส่งผลต่อประสิทธิภาพการใช้งานของวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพแบบรูปตัวการ์ตูนซึ่งอาจเป็นไปได้ว่า เมื่อเวลาผ่านไปนานกว่า 15 วัน ผลการทดลองจะเห็นผลที่ชัดเจนมากขึ้นกว่านี้

2) ทำการเพิ่มตัวแปรควบคุม (Control Variable) ในการทดลอง เช่น กำหนดให้ห้ามใช้ตัวการ์ตูนซ้ำกันเกินกว่าที่ตัวในการสร้างรหัสผ่าน เพื่อป้องกันผู้เข้าร่วมการทดลองจงใจตั้งรหัสผ่านที่จดจำง่ายเกินไป

3) ทำการทดลองทางด้านความปลอดภัย โดยทดลอง

เปรียบเทียบวิธีการโจมตีระบบวิธีการอื่นนอกจากวิธีการ Shoulder surfing เช่น Brute force attack, Spyware, Social engineering เพื่อหารูปแบบการพิสูจน์ตัวตนที่มีความปลอดภัย

7. เอกสารอ้างอิง

- [1] A. Adams and M. A. Sasse. "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures." *Communications of the ACM*, Vol. 42, pp. 41-46, 1999.
- [2] D. Feldmeier and P. Karn. "UNI× password security-Ten years later." In *Proceedings of the 19th International Conference on Advances in Cryptology (CRYPTO '89)*. Lecture Notes in Computer Science, Vol. 435. Springer Verlag, 1989.
- [3] R. Morris and K. Thompson. "Password security: A case history." *Communications of the ACM (11)*, pp. 594-597, 1979.
- [4] T. Wu. "A real-world analysis of Kerebros password security." In *Proceedings of the 1999ISOC Symposium on Network and Distributed System Security*. 9, Vol. 8, pp. 723-736, 1990.
- [5] M. Kotadia. "Microsoft: Write down your passwords." in *ZDNet Australia*, 23 May, 2005.
- [6] R. Dhamija and A. Perrig. "Deja Vu: A User Study Using Images for Authentication." In *Proceedings of 9th USENIX Security Symposium*, 2000.
- [7] A. Paivio, T. B. Rogers and P. C. Smythe. "Why are pictures easier to recall than words?" *Psychonomic Science*, pp. 11:137-138, 1968.
- [8] G. H. Bower, M. B. Karlin and A. Dueck. "Comprehension and memory for pictures." *Memory and Cognition* 3, pp. 216-220, 1975.
- [9] L. Standing. "Learning 10,000 picture." *Quarterly Journal of Experimental Psychology*, pp. 25:207-222, 1973.
- [10] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin. "The Design and Analysis of Graphical



- Passwords.” *In Proceedings of the 8th USENIX Security Symposium*, 1999.
- [11] J. Thorpe and P. C. V. Oorschot. “Towards Secure Design Choices for Implementing Graphical Passwords.” *In 20th Annual Computer Security Applications Conference (ACSAC)*. Tucson, USA: IEEE, 2004.
- [12] H. Tao, C. Adams. “Pass-Go: A Proposal to Improve the Usability of Graphical Passwords. ” *International Journal of Network Security*, Vol. 7, Issue 2, pp. 273-292, 2006.
- [13] C. Hinds and C. Ekwueme. “Increasing security and usability of computer systems with graphical password.” *In Proceedings of the 45th annual southeast regional conference, ACM-SE*, NY, USA, 2007.
- [14] วัชรินทร์ มธุรสพงศ์พันธ์ และ ณัฐธนนท์ หงส์วิทธิธร, “การศึกษาการใช้งานได้ของรหัสผ่านรูปภาพบนตารางกริด.” *In Proceedings of the 4th International Conference on Knowledge and Smart Technology (KST)*, 2012.

