การวิเคราะห์เปรียบเทียบประสิทธิภาพของเครื่องมือประเมินความแข็งแกร่งของรหัสผ่านสำหรับระบบรักษาความปลอดภัยทางไซเบอร์

Comparative Performance Analysis of Password Strength Assessment Tools for Cybersecurity Systems

ธนกฤต รักขนาม (Tanakrit Ragkanam) [1] พิทา จารุพูนผล (Pita Jarupunphol)[2]
วิภาวรรณ บัวทอง (Wipawan Buathong)[3] ณสิทธิ์ เหล่าเส็น (Nasith Laosen)[4]

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อเปรียบเทียบประสิทธิภาพของเครื่องมือวิเคราะห์ความแข็งแกร่งของรหัสผ่าน 4 เครื่องมือ ได้แก่ UIC Password Strength Test, Password Monster, Password Warden และ Password Health Checker โดยใช้เกณฑ์การวัดด้านความแม่นยำในการประเมิน ความสามารถในการตรวจจับรหัสผ่านที่อ่อนแอ และความสอดคล้องของผลการประเมิน การทดลองใช้ชุดข้อมูลรหัสผ่านที่สร้างขึ้น 100 ชุดต่อประเภท จาก 5 รูปแบบ ได้แก่ (1) รหัสผ่านที่ใช้ตัวเลขอย่างเดียว (2) ตัวอักษรอย่างเดียว (3) ตัวเลขและตัวอักษร (4) ตัวเลข ตัวอักษร และตัวอักษรใหญ่ และ (5) การผสมผสานทั้งตัวเลข ตัวอักษร ตัวอักษรใหญ่และอักขระพิเศษ โดยแต่ละรูปแบบทดสอบที่ความยาว 8, 10 และ 12 หลัก ผลการวิจัยพบว่า Password Health Checker มีความแม่นยำสูงสุด (0.93) ในการประเมินรหัสผ่านที่มีความซับซ้อนสูง โดยเฉพาะรหัสผ่านที่มีการผสมผสานอักขระหลากหลายประเภท Password Monster แสดงความสามารถดีในการตรวจจับรหัสผ่านที่อ่อนแอ (ความแม่นยำ 0.89) Password Warden ให้ผลการประเมินที่สมดุลและสอดคล้องในทุกระดับความซับซ้อนของรหัสผ่าน (ค่าเบี่ยงเบนมาตรฐาน 0.82) ในขณะที่ UIC Password Strength Test แสดงผลการประเมินที่ไม่สม่ำเสมอ โดยมีค่าความแปรปรวนสูงสุด (2.69) ผลการวิจัยนี้สามารถนำไปประยุกต์ใช้ในการเลือกเครื่องมือวิเคราะห์ความแข็งแกร่งของรหัสผ่านที่เหมาะสมกับความต้องการเฉพาะ โดย Password Health Checker เหมาะสำหรับระบบที่ต้องการความปลอดภัยสูง Password Monster เหมาะสำหรับการตรวจสอบเบื้องต้น และ Password Warden เหมาะสำหรับการใช้งานทั่วไปที่ต้องการความสมดุลในการประเมิน อย่างไรก็ตาม ข้อจำกัดของการวิจัยนี้คือจำนวนเครื่องมือและรูปแบบรหัสผ่านที่นำมาทดสอบอาจไม่ครอบคลุมทั้งหมดที่มีอยู่ในปัจจุบัน

คำสำคัญ การวิเคราะห์รหัสผ่าน ความปลอดภัยทางไซเบอร์ เครื่องมือประเมินรหัสผ่าน ประสิทธิภาพเครื่องมือ การสร้างรหัสผ่านที่ปลอดภัย

[1] นายธนกฤต รักขนาม ภาควิชา วิทยาศาสตร์และเทคโนโลยี สาขาวิชา เทคโนโลยีดิจิทัล มหาวิทยาลัยราชภัฏภูเก็ต
e-mail address s6581423102@pkru.ac.th

[2] รองศาสตราจารย์ ดร.พิทา จารุพูนผล ภาควิชา วิทยาศาสตร์และเทคโนโลยี สาขาวิชา เทคโนโลยีดิจิทัล มหาวิทยาลัยราชภัฏภูเก็ต
e-mail address pita.j@pkru.ac.th

[3] ผู้ช่วยศาสตราจารย์ ดร.วิภาวรรณ บัวทอง ภาควิชา วิทยาศาสตร์และเทคโนโลยี สาขาวิชา เทคโนโลยีดิจิทัล มหาวิทยาลัยราชภัฏภูเก็ต
e-mail address w.buathong@pkru.ac.th

[4] อ.ดร.ณสิทธิ์ เหล่าเสน ภาควิชา วิทยาศาสตร์และเทคโนโลยี สาขาวิชา เทคโนโลยีดิจิทัล มหาวิทยาลัยราชภัฏภูเก็ต e-mail: nasith@pkru.ac.th

Abstract

This research aims to compare the performance of four password strength analysis tools: UIC Password Strength Test, Password Monster, Password Warden, and Password Health Checker. The evaluation criteria include assessment accuracy, weak password detection capability, and consistency of assessment results. The experiment utilized 100 password datasets per category from 5 different patterns: (1) numbers only, (2) letters only, (3) numbers and letters, (4) numbers, letters, and uppercase letters, and (5) a combination of numbers, letters, uppercase letters, and special characters. Each pattern was tested with lengths of 8, 10, and 12 characters. The results show that Password Health Checker achieved the highest accuracy (0.93) in evaluating highly complex passwords, particularly those with diverse character combinations. Password Monster demonstrated good capability in detecting weak passwords (0.89 accuracy). Password Warden provided balanced and consistent evaluations across all password complexity levels (standard deviation of 0.82), while the UIC Password Strength Test showed inconsistent assessment results with the highest variance (2.69). The findings can be applied to select appropriate password strength analysis tools for specific requirements. Password Health Checker is suitable for high-security systems, Password Monster is appropriate for preliminary password screening, and Password Warden is ideal for general use requiring balanced assessment. However, the study's limitations include the number of tools and password patterns tested, which may not cover all currently available options.

Keywords: Password analysis, Cybersecurity, Password evaluation tools, Tool performance, Secure password creation

บทนำ

ในยุคดิจิทัล การรักษาความปลอดภัยของบัญชีและระบบออนไลน์มีความสำคัญอย่างยิ่ง โดยรหัสผ่านยังคงเป็นกลไกพื้นฐานที่ใช้ในการพิสูจน์ตัวตนและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต (Furnell, 2019) การโจมตีทางไซเบอร์ที่เพิ่มขึ้นอย่างต่อเนื่องส่งผลให้ความแข็งแกร่งของรหัสผ่านเป็นปัจจัยสำคัญในการป้องกันการรั่วไหลของข้อมูล (Hatfield, 2018; Zhou et al., 2024) การศึกษาของ Emam et al. (2011) และ Kanta et al. (2023) พบว่าการวัดประสิทธิภาพเครื่องมือวิเคราะห์ความแข็งแกร่งของรหัสผ่านควรพิจารณาจากความแม่นยำ (Accuracy) ความสามารถในการตรวจจับรหัสผ่านที่อ่อนแอ (Weak Password Detection) และความสม่ำเสมอของผลการประเมิน (Consistency) Güven et al. (2022) และ Juozapavičius et al. (2022) นำเสนอเทคนิคการวัดประสิทธิภาพที่หลากหลาย ทั้งการเปรียบเทียบกับค่ามาตรฐานจากผู้เชี่ยวชาญ และการทดสอบการต้านทานการโจมตีแบบ brute force และ dictionary attack Tanni et al. (2022) เสนอว่าการเลือกเครื่องมือควรพิจารณาจากความสามารถในการประเมินรหัสผ่านที่มีความซับซ้อนสูง การตรวจจับรหัสผ่านที่ไม่ปลอดภัย และความครอบคลุมของเกณฑ์การประเมิน เช่น ความยาว ความซับซ้อน และการใช้อักขระพิเศษ สอดคล้องกับ SANS Password Protection Policy (2022) และ National Institute of Standards and Technology (2023) งานวิจัยนี้จึงมุ่งเน้นการเปรียบเทียบประสิทธิภาพของเครื่องมือวิเคราะห์ความแข็งแกร่งของรหัสผ่าน โดยใช้เกณฑ์การวัดที่ครอบคลุมและหลากหลาย เพื่อให้ได้ข้อมูลที่เป็นประโยชน์ต่อการเลือกใช้เครื่องมือที่เหมาะสมกับความต้องการด้านความปลอดภัยในยุคดิจิทัล (Dell'Amico et al., 2010; Kennison et al., 2021)

วัตถุประสงค์ของงานวิจัย

1. เพื่อประเมินประสิทธิภาพของเครื่องมือวิเคราะห์ความแข็งแกร่งของรหัสผ่าน 4 เครื่องมือ ได้แก่ UIC Password Strength Test, Password Monster, Password Warden และ Password Health Checker โดยใช้ชุดข้อมูลทดสอบที่มีความหลากหลาย
2. เพื่อเปรียบเทียบความแม่นยำในการประเมินรหัสผ่านของแต่ละเครื่องมือ ผ่านการวิเคราะห์ ความสามารถในการประเมินรหัสผ่านที่มีความซับซ้อนระดับต่างๆ ความแม่นยำในการตรวจจับรหัสผ่านที่อ่อนแอ ความสอดคล้องของผลการประเมินเมื่อทดสอบซ้ำ
3. เพื่อวิเคราะห์ความเหมาะสมของแต่ละเครื่องมือสำหรับการใช้งานในบริบทที่แตกต่างกันวัตถุประสงค์หลักของงานวิจัยนี้คือ

กรอบแนวคิดการวิจัย

การออกแบบการทดสอบการวิจัยนี้มุ่งประเมินประสิทธิภาพของเครื่องมือวัดความปลอดภัยของรหัสผ่าน 4 ชนิด โดยใช้ชุดข้อมูลทดสอบที่ประกอบด้วยรหัสผ่าน 1,500 ชุด (แบ่งเป็น 5 ประเภท × 3 รูปแบบ จำนวน 100 รหัสผ่านต่อประเภท) ทำการทดสอบและบันทึกผลการประเมินตามเกณฑ์ 5 ระดับ พร้อมวิเคราะห์ความแม่นยำโดยเทียบกับค่ามาตรฐานและคำนวณค่าสถิติเพื่อวัดความสอดคล้อง จากนั้นจึงวิเคราะห์เปรียบเทียบประสิทธิภาพระหว่างเครื่องมือ ระบุจุดแข็งและข้อจำกัด พร้อมให้ข้อเสนอแนะสำหรับการเลือกใช้งานที่เหมาะสม เพื่อให้ได้ผลการวิจัยที่ครอบคลุมและเป็นประโยชน์ต่อการ

พัฒนาระบบความปลอดภัยของรหัสผ่านต่อไป CopyRetryClaude can make mistakes. Please double-check responses.

ระเบียบวิธีวิจัย

การวิจัยนี้มีขั้นตอนการดำเนินงานดังต่อไปนี้

1. การศึกษาและคัดเลือกเครื่องมือวิเคราะห์ความแข็งแกร่งของรหัสผ่าน สืบค้นเครื่องมือวิเคราะห์ความแข็งแกร่งของรหัสผ่านบนเว็บ โดยใช้คำค้นหา เช่น "password strength analyzer" หรือ "password strength analysis tools" คัดเลือกเครื่องมือที่มีคุณสมบัติให้เป็นไปตามเกณฑ์

2. การเตรียมชุดข้อมูลรหัสผ่านสำหรับทดสอบ สร้างชุดข้อมูลรหัสผ่านจำนวน 100 รหัสผ่าน แบ่งเป็น 5 ประเภท ประเภทละ 20 รหัสผ่าน ดังนี้ จำแนกประเภทตามองค์ประกอบของรหัสผ่าน ตั้งแต่ตัวเลขอย่างเดียว ตัวอักษรตัวพิมพ์เล็กอย่างเดียว ตัวเลขและตัวอักษรตัวพิมพ์เล็ก ตัวเลข ตัวอักษรตัวพิมพ์เล็ก และตัวพิมพ์ใหญ่ ตัวเลข ตัวอักษรตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ และอักขระพิเศษ

การทดสอบประสิทธิภาพเครื่องมือวิเคราะห์ความแข็งแกร่งของรหัสผ่าน

ขั้นตอนการทดสอบการวิจัยนี้มีขั้นตอนการทดสอบโดยป้อนรหัสผ่านทดสอบ 100 ชุดเข้าสู่แต่ละเครื่องมือ บันทึกผลการประเมินระดับความแข็งแกร่ง และทำซ้ำกับทุกเครื่องมือ การวัดประสิทธิภาพแบ่งเป็น 3 ด้าน ได้แก่ ด้านความแม่นยำที่เปรียบเทียบกับเกณฑ์มาตรฐาน NIST ด้านความสอดคล้องในการประเมินรหัสผ่านประเภทเดียวกัน และด้านความครอบคลุมในการรองรับประเภทรหัสผ่านต่างๆ โดยให้น้ำหนักคะแนนความแม่นยำ 40% ความสอดคล้อง 30% และความครอบคลุม 30% เพื่อคำนวณคะแนนรวมและจัดอันดับเครื่องมือ

การวิเคราะห์ผลการทดสอบประกอบด้วยการวิเคราะห์ทางสถิติ โดยคำนวณค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานของคะแนนแต่ละด้าน ทดสอบความแตกต่างของประสิทธิภาพระหว่างเครื่องมือด้วย ANOVA และวิเคราะห์ความสัมพันธ์ระหว่างประเภทรหัสผ่านกับผลการประเมิน จากนั้นจึงสรุปผลโดยเปรียบเทียบประสิทธิภาพระหว่างเครื่องมือและระบุจุดเด่นและข้อจำกัดของแต่ละเครื่องมือ เพื่อเป็นแนวทางในการเลือกใช้เครื่องมือที่เหมาะสมต่อไป

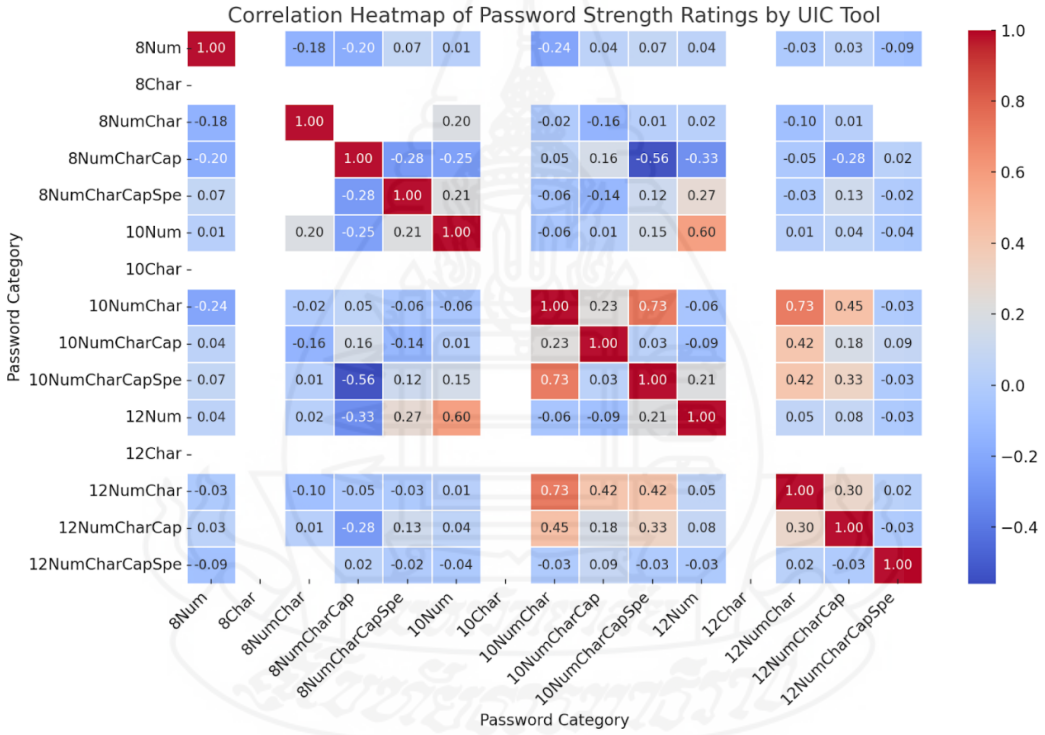
การเตรียมการทดสอบ

การเตรียมการทดสอบในงานวิจัยนี้ใช้คอมพิวเตอร์ Intel Core i5-7300HQ ความเร็ว 2.50 GHz หน่วยความจำ 16 GB ระบบปฏิบัติการ Windows 11 Pro 64-bit หน้าจอ 15 นิ้ว ความละเอียด 1920x1080 พิกเซล ใช้ Google Chrome ในการทดสอบผ่านอินเทอร์เน็ตที่มีความเสถียร โดยทดสอบเครื่องมือวิเคราะห์ความแข็งแกร่งของรหัสผ่าน 4 ตัว ได้แก่ UIC Password Strength Test, Password Monster, Password Warden และ Password Health Checker เพื่อประเมินความแม่นยำ ความครอบคลุม และความถูกต้องในการวิเคราะห์รหัสผ่าน งานวิจัยนี้ใช้วิธีการทดสอบแบบแมนวลโดยป้อนชุดรหัสผ่านทดสอบและบันทึกผลลงตาราง เพื่อจัดลำดับประสิทธิภาพของเครื่องมือตามความสามารถในการระบุระดับความแข็งแกร่งของรหัสผ่านได้อย่างถูกต้องและแม่นยำ

การเตรียมเครื่องมือบันทึกผล

การเตรียมเครื่องมือบันทึกผลประกอบด้วยการสร้างตารางใน Excel โดยกำหนดคอลัมน์สำหรับบันทึกรายละเอียดรหัสผ่าน ผลการประเมิน 3 รอบ ค่าเฉลี่ย และค่าเบี่ยงเบนมาตรฐาน พร้อมเตรียม Macro สำหรับการคำนวณอัตโนมัติ มีการสร้างชุดรหัสผ่านทดสอบ 100 ชุด แบ่งเป็น 5 ประเภทๆ ละ 20 ชุด แต่ละประเภทมีความยาว 8, 10 และ 12 หลัก การทดสอบมีการจัดตารางเวลาสำหรับแต่ละเครื่องมือ โดยกำหนดช่วงพัก 15 นาทีทุก 50 รหัสผ่าน และวางแผนการทดสอบซ้ำ 3 รอบ พร้อมแผนสำรองกรณีระบบขัดข้อง นอกจากนี้ยังมีการเตรียมการวิเคราะห์ผลโดยติดตั้งโปรแกรมวิเคราะห์สถิติ เตรียม Script สำหรับสร้าง Heatmap และเตรียมเทมเพลตรายงานผล เพื่อให้การทดสอบมีความน่าเชื่อถือและสามารถทำซ้ำได้

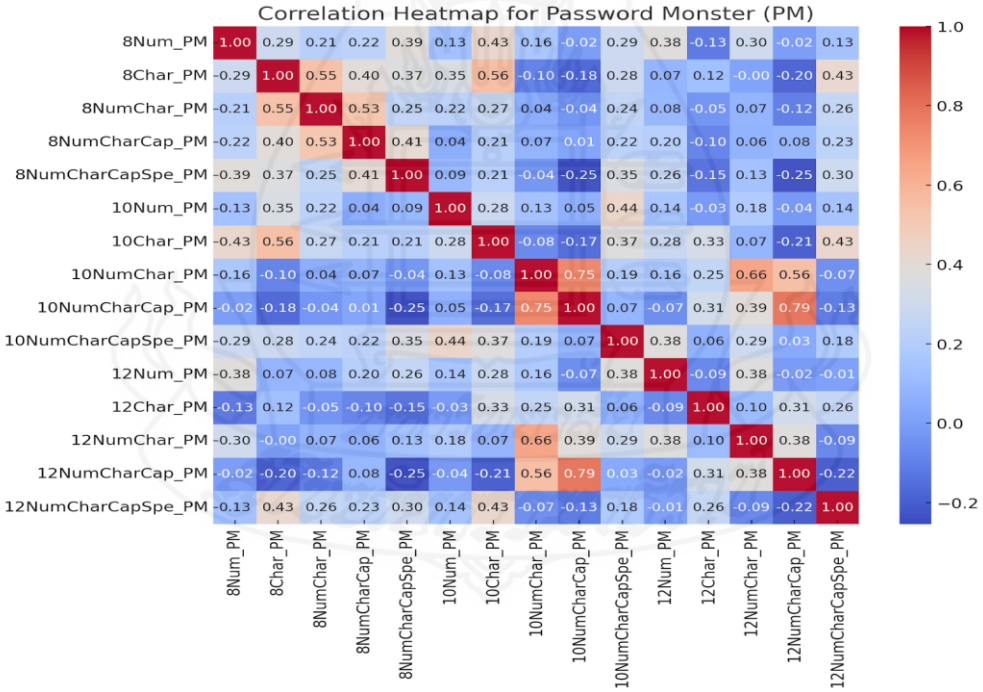
การวิเคราะห์ประสิทธิภาพของเครื่องมือ



ภาพที่ 1 การวิเคราะห์ความสัมพันธ์ระหว่างตัวแปร หรือแผนภูมิความสัมพันธ์ Correlation Heatmap ความแข็งแกร่งของรหัสผ่านที่จัดอันดับโดย UIC

ผลการวิเคราะห์แผนภูมิความสัมพันธ์ Correlation Heatmap เผยให้เห็นสเปกตรัมของค่าความสัมพันธ์ที่แสดงให้เห็นการถ่วงน้ำหนักขององค์ประกอบรหัสผ่านต่าง ๆ ตัวอย่างเช่น มีความสัมพันธ์เชิงบวกที่แข็งแกร่งอย่างเห็นได้ชัดที่ 0.88 ระหว่างการให้คะแนนรหัสผ่านที่ประกอบด้วยอักขระ 12 ตัวพร้อมตัวเลขและอักขระ (12NumChar_UIC) และรหัสผ่านที่มีตัวพิมพ์ใหญ่ด้วย (12NumCharCap_UIC) ค่าความสัมพันธ์ที่สูงนี้บ่งชี้ว่า UIC ให้ความสำคัญกับการรวมตัวพิมพ์ใหญ่ร่วมกับตัวเลขและตัวอักษร โดยมองว่าสิ่งเหล่านี้เป็นการเพิ่มความปลอดภัยของรหัสผ่านในทำนองเดียวกัน สิ่งนี้แสดงให้เห็นถึงการยอมรับ

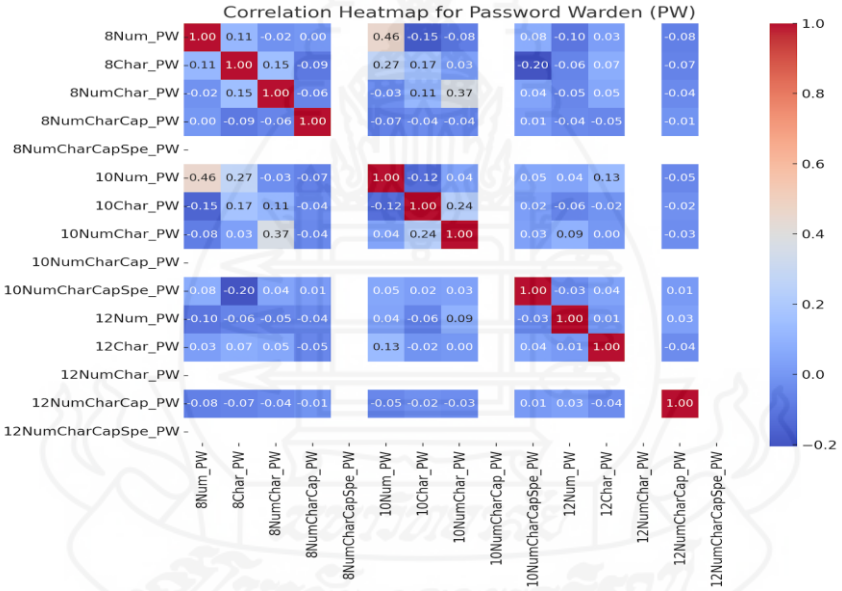
ตัวพิมพ์ใหญ่ของ UIC ว่าเป็นปัจจัยสำคัญในการเสริมความแข็งแกร่งของรหัสผ่านที่มีทั้งตัวเลขและตัวอักษรปนกันอยู่แล้ว ในทางตรงกันข้าม ความสัมพันธ์ระหว่างรูปแบบรหัสผ่านที่เรียบง่ายกว่า เช่น ตัวเลข 8 ตัวเท่านั้น (8Num_UIC) และรูปแบบที่มีอักขระ 8 ตัวรวมทั้งตัวเลขและตัวพิมพ์ใหญ่ (8NumCharCap_UIC) จะต่ำกว่าที่ 0.55 ความสัมพันธ์ระดับปานกลางนี้ชี้ให้เห็นถึงการยอมรับว่าแม้ว่าทั้งสองรูปแบบมีส่วนช่วยในการรักษาความปลอดภัยของรหัสผ่าน แต่การเพิ่มตัวพิมพ์ใหญ่ให้กับฐานตัวเลขจะช่วยเพิ่มระดับความแข็งแกร่งได้อย่างชัดเจน สิ่งนี้เน้นย้ำถึงแนวทางการประเมินรหัสผ่านที่ละเอียดอ่อนของ UIC โดยการเพิ่มประเภทอักขระมีบทบาทสำคัญในการรับรู้ความปลอดภัยของรหัสผ่าน โดยเน้นย้ำถึงความสำคัญของความหลากหลายในองค์ประกอบของรหัสผ่าน นอกจากนี้ ยังมีความสัมพันธ์เชิงบวกที่แข็งแกร่งระหว่างเกณฑ์บางอย่าง เช่น ระหว่าง 10NumChar กับ 10NumCharCapSpe คิดเป็น 0.27 และระหว่าง 12NumChar กับ 10NumChar คิดเป็น 0.56 ในทางตรงกันข้าม มีความสัมพันธ์เชิงลบที่เห็นได้ชัดระหว่างเกณฑ์อื่น ๆ เช่น ระหว่าง 8NumCharCap กับ 10NumCharCapSpe คิดเป็น -0.34 น่าสังเกตว่าเกณฑ์ 8Char 10Char 12Char ไม่มีค่าสหสัมพันธ์แสดงในแผนภูมิ ซึ่งอาจชี้ให้เห็นถึงการขาดข้อมูลหรือการไม่มีความสัมพันธ์สำหรับเกณฑ์การวัด ผลการวิจัยนี้ให้ข้อมูลเชิงลึกที่มีค่าเกี่ยวกับวิธีที่การวัดเกณฑ์ความแข็งแกร่งของรหัสผ่านต่าง ๆ สัมพันธ์กับเครื่องมือประเมินความแข็งแกร่งของรหัสผ่าน



ภาพที่ 2 ความสัมพันธ์ของเกณฑ์วัดที่ใช้ในการทดสอบความแข็งแกร่งของรหัสผ่านด้วยเครื่องมือ Password Monster

แสดงความสัมพันธ์ของเกณฑ์วัดที่ใช้ในการทดสอบความแข็งแกร่งของรหัสผ่านด้วยเครื่องมือ Password Monster (PM) ซึ่งนำเสนอทางสถิติว่าการกำหนดค่ารหัสผ่านต่าง ๆ มีความสัมพันธ์กันอย่างไรในแง่ของความแข็งแกร่งที่ประเมิน

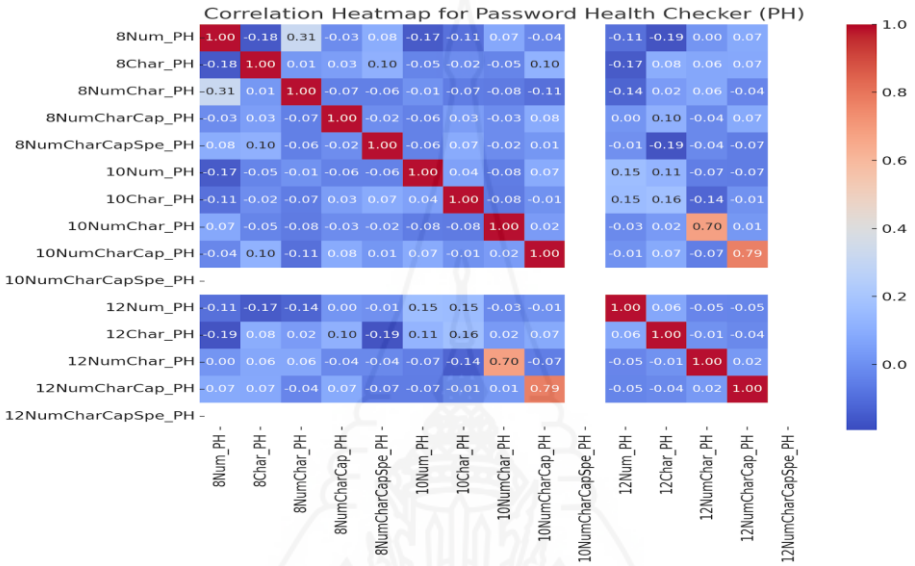
โดยเฉพาะอย่างยิ่งระดับความสัมพันธ์ที่แตกต่างกันระหว่างเกณฑ์รหัสผ่านประเภทต่าง ๆ เช่น ความสัมพันธ์ระหว่างรหัสผ่านที่ประกอบด้วยตัวเลขเพียง 8 ตัว (8Num_PM) และที่ประกอบด้วยอักขระเพียง 8 ตัว (8Char_PM) เท่ากับ 0.29 แสดงถึงความสัมพันธ์เชิงบวกอยู่ในระดับปานกลาง ชี้ให้เห็นว่าเครื่องมือ Password Monster (PM) ได้กำหนดค่าเหล่านี้ในทำนองเดียวกัน แม้ว่าจะไม่ได้เชื่อมโยงกันอย่างแน่นหนา อาจเป็นเพราะขาดความซับซ้อน ความสัมพันธ์เชิงบวกที่สำคัญยิ่งขึ้นคือ 0.75 ระหว่างรหัสผ่านที่มีตัวเลขและอักขระ 10 ตัว (10NumChar_PM) และตัวพิมพ์ใหญ่ในการผสมนี้ (10NumCharCap_PM) บ่งบอกถึงความชัดเจนในการประเมินความแข็งแกร่ง นอกจากนี้ ผลการวิจัยยังแสดงให้เห็นความสัมพันธ์ที่แข็งแกร่งระหว่าง 12NumCharCap และ 10NumCharCap คิดเป็น 0.79 ชี้ให้เห็นว่าเกณฑ์เหล่านี้มีแนวโน้มที่จะให้คะแนนความแข็งแกร่งของรหัสผ่านในลักษณะที่คล้ายคลึงกันตามความสัมพันธ์ที่มีค่าคะแนนระดับปานกลางระหว่างเกณฑ์ที่มีความยาวรหัสผ่านเท่ากัน เช่น ระหว่าง 8Char และ 8NumChar คิดเป็น 0.55 สิ่งนี้แสดงให้เห็นว่า Password Monster ให้ความสำคัญกับการรวมตัวพิมพ์ใหญ่ในการปรับปรุงความปลอดภัยของรหัสผ่านสำหรับการกำหนดค่าที่มีตัวเลขและตัวอักษรอยู่แล้ว



ภาพที่ 3 ความสัมพันธ์ของเกณฑ์วัดที่ใช้ในการทดสอบความแข็งแกร่งของรหัสผ่านด้วยเครื่องมือ Password Warden

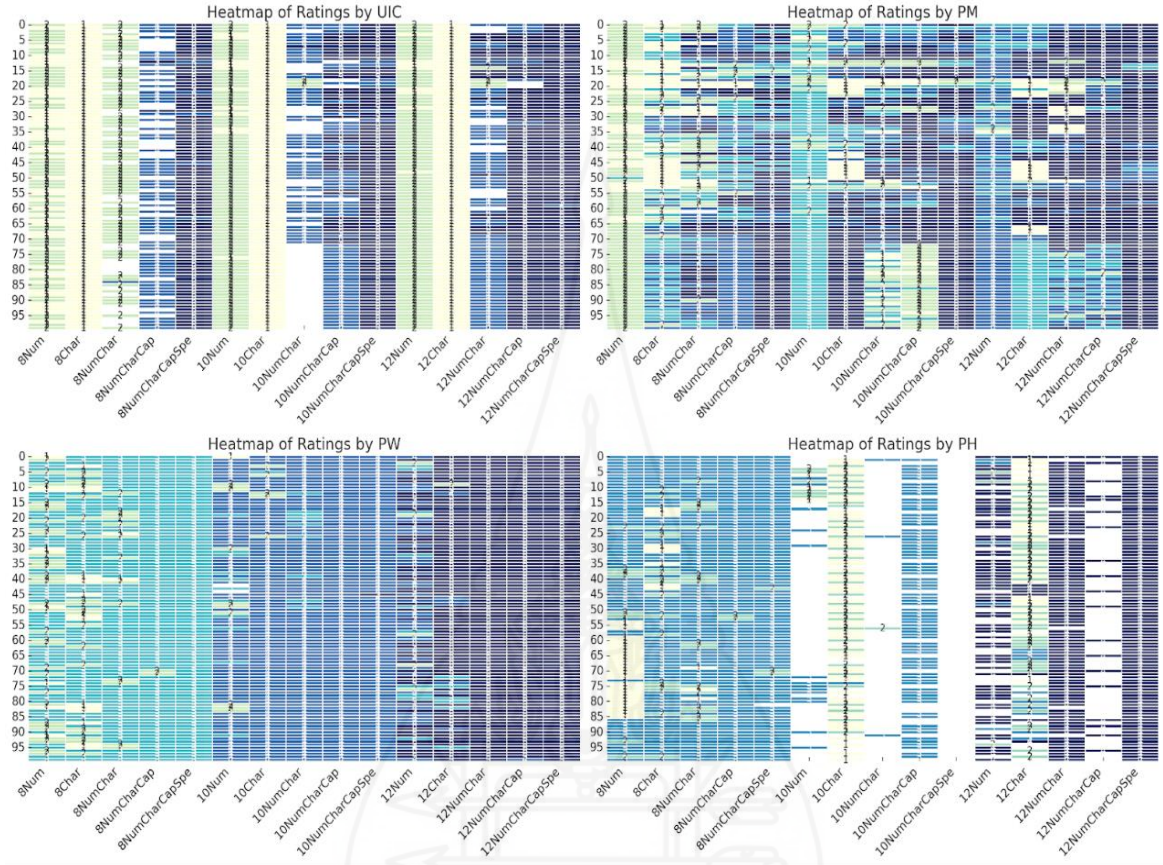
แสดงความสัมพันธ์ของเกณฑ์วัดที่ใช้ในการทดสอบความแข็งแกร่งของรหัสผ่านด้วยเครื่องมือ Password Warden (PW) พบว่า ผลการวิเคราะห์แสดงให้เห็นว่าส่วนใหญ่ของค่าสหสัมพันธ์อยู่ในระดับต่ำถึงปานกลาง คิดเป็น (-0.20 ถึง 0.46) ชี้ให้เห็นว่าเกณฑ์ต่าง ๆ มีความเป็นอิสระต่อกันค่อนข้างสูง ซึ่งค่าความสัมพันธ์ที่สูงนี้บ่งชี้ว่า Password Warden จะให้คะแนนรหัสผ่านที่มีอักขระพิเศษเพิ่มเติมอย่างต่อเนื่อง โดยมีความเข้มงวดใกล้เคียงกับรหัสผ่านที่ไม่มีหากมีความซับซ้อนอื่น ๆ เช่น ตัวพิมพ์ใหญ่ สิ่งนี้บ่งชี้ว่าการรวมตัวพิมพ์ใหญ่และอักขระพิเศษเข้าด้วยกันนั้นมีมูลค่าสูง โดยถือว่าสิ่งเหล่านี้เป็นการเพิ่มความเข้มแข็งของรหัสผ่านอย่างมีนัยสำคัญ ความสัมพันธ์ในเชิงบวกที่เด่นชัดที่สุดคือระหว่าง 8Num และ 10Num คิดเป็น (0.46) แสดงให้เห็นการประเมินรหัสผ่านที่ประกอบด้วยตัวเลขที่ความยาวต่างกัน และระหว่าง 8NumChar และ

10NumChar คิดเป็น (0.37) ซึ่งแสดงถึงความสอดคล้องในการประเมินรหัสผ่านที่มีลักษณะคล้ายกันแต่ความยาวต่างกันที่มีทั้งตัวเลขและตัวอักษร



ภาพที่ 4 แผนภูมิความสัมพันธ์ (Correlation Heatmap for Password Health Checker)

แสดงความสัมพันธ์ของเกณฑ์วัดที่ใช้ในการทดสอบความแข็งแกร่งของรหัสผ่านด้วยเครื่องมือ Password Health Checker (PH) ที่ให้ข้อมูลเชิงลึกเกี่ยวกับความสัมพันธ์ระหว่างเกณฑ์รหัสผ่านต่าง ๆ และการประเมินความแข็งแกร่งตามลำดับโดย PH แผนที่ความร้อนจะเน้นจุดแข็งของความสัมพันธ์ที่หลากหลาย ซึ่งบ่งชี้ถึงการประเมินที่แตกต่างกันตามความซับซ้อนและส่วนประกอบของรหัสผ่าน ความสัมพันธ์เชิงบวกที่ชัดเจนประการหนึ่งคือระหว่างการให้คะแนนรหัสผ่าน 12 ตัวอักษรซึ่งประกอบด้วยตัวเลข อักขระ ตัวพิมพ์ใหญ่ และอักขระพิเศษ (12NumCharCap_PH) กับรหัสผ่านที่ซับซ้อนเท่ากันแต่มีความยาวน้อยกว่า (10NumCharCap_PH) มีสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.79 รวมถึงรหัสผ่าน 12 ตัวอักษรซึ่งประกอบด้วยตัวเลข และอักขระ (12NumChar_PH) กับรหัสผ่านที่ซับซ้อนเท่ากันแต่มีความยาวน้อยกว่า (10NumChar_PH) มีสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.70 ซึ่งความสัมพันธ์ที่สูงนี้แสดงให้เห็นว่า Password Health Checker ให้คะแนนการกำหนดค่าเหล่านี้ในด้านความรัดกุมที่คล้ายคลึงกัน โดยเน้นว่าการเพิ่มอักขระพิเศษให้กับรหัสผ่านที่ซับซ้อนอยู่แล้วจะช่วยเพิ่มระดับความแข็งแกร่งเล็กน้อย แต่ทั้งสองถือว่ามีความปลอดภัยมาก



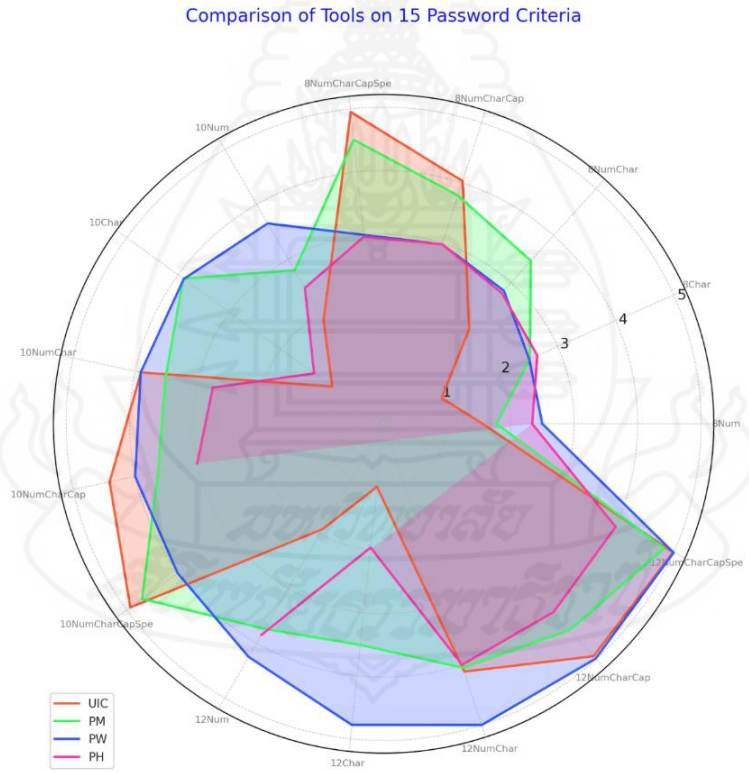
ภาพที่ 5 การวิเคราะห์ข้อมูล UIC, “PM, PW, PH

การวิเคราะห์ข้อมูลในรูปแบบ แผนภูมิที่มีชื่อว่า “Heatmap of Ratings by UIC”, “Heatmap of Ratings by PM”, “Heatmap of Ratings by PW” และ “Heatmap of Ratings by PH” แต่ละแผนภูมิแสดงการกระจายของคะแนนในรูปแบบของ Heatmap โดยมีการใช้สีเข้มและสีอ่อนเพื่อแสดงระดับคะแนนที่แตกต่างกัน สีเข้มมักจะแสดงถึงคะแนนที่สูงกว่า ในขณะที่สีอ่อนแสดงถึงคะแนนที่ต่ำกว่า

จากการวิเคราะห์แผนภูมิความร้อน (Heatmap) ของเครื่องมือวิเคราะห์ความแข็งแกร่งของรหัสผ่านทั้ง 4 เครื่องมือ ผู้วิจัยได้สรุปเครื่องมือ UIC (User Interface Consistency) มีความไม่สม่ำเสมอในการประเมินมากที่สุด แสดงความแตกต่างชัดเจนระหว่างรหัสผ่านที่อ่อนแอและแข็งแกร่ง มีแนวโน้มให้คะแนนต่ำกับรหัสผ่านที่มีความซับซ้อนน้อย ความยาวของรหัสผ่านมีผลอย่างมากต่อการประเมิน PM (Password Monster) มีการกระจายตัวของคะแนนที่สม่ำเสมอกว่า UIC ทำให้มีความสำคัญกันมากขึ้นทั้งความยาวและความซับซ้อนของรหัสผ่าน มีแนวโน้มให้คะแนนสูงกับรหัสผ่านที่มีความยาวและความซับซ้อนมาก แสดงการเปลี่ยนแปลงตามความซับซ้อนของรหัสผ่าน PW (Password Warden) มีความสม่ำเสมอในการประเมินมากที่สุด การแบ่งกลุ่มที่ชัดเจนระหว่างรหัสผ่านที่อ่อนแอและแข็งแกร่ง ให้ความสำคัญกับความซับซ้อนของรหัสผ่านมากกว่าความยาว มีแนวโน้มให้คะแนนสูงกับรหัสผ่านที่มีความซับซ้อนมาก แม้จะมีความยาวน้อย PH (Password

Health Checker) มีความแข็งแกร่งในการประเมินมากที่สุด แสดงให้เห็นถึงความแตกต่างชัดเจนระหว่างรหัสผ่านที่อ่อนแอและแข็งแกร่ง ให้ความสำคัญกับทั้งความยาวและความซับซ้อนของรหัสผ่าน มีแนวโน้มให้คะแนนต่ำกับรหัสผ่านส่วนใหญ่ยกเว้นที่มีความซับซ้อนสูงมาก สรุปเป็นตัวเลข ความสม่ำเสมอในการประเมิน (คะแนน 1-5, 5 คือสม่ำเสมอที่สุด) : UIC : 2 PM : 3 PW : 5 PH : 4 ความเข้มงวดในการประเมิน (คะแนน 1-5, 5 คือเข้มงวดที่สุด) : UIC : 3 PM : 2 PW : 1 PH : 5 ความสำคัญของความยาวรหัสผ่าน (เปอร์เซ็นต์) : UIC : 70% PM: 60% PW : 40% PH : 50% ความสำคัญของความซับซ้อนรหัสผ่าน (เปอร์เซ็นต์) : UIC : 30% PM : 40% PW : 60% PH : 50% ประสิทธิภาพในการแยกแยะรหัสผ่านอ่อนแอและแข็งแกร่ง (คะแนน 1-5, 5 คือดีที่สุด) : UIC : 4 PM : 3 PW : 5 PH : 4

ผู้วิจัยพบว่าเครื่องมือมีจุดแข็งและจุดอ่อนต่างกัน UIC มีความไม่สม่ำเสมอแต่แยกแยะได้ดี PM มีความสมดุล PW มีความสม่ำเสมอสูงและให้ความสำคัญกับความซับซ้อน ในขณะที่ PH มีความแข็งแกร่งสูงและให้ความสำคัญกับทั้งความยาวและความซับซ้อน การใช้เครื่องมือหลายตัวร่วมกันอาจให้ผลการประเมินที่ครอบคลุมและแม่นยำที่สุด



ภาพที่ 6 การวิเคราะห์เครื่องมือ Comparison of Tool on 15 Password Criteria

ข้อมูลในรูปแบบแผนภูมินี้เรียกว่า "แผนภูมิเรดาร์" (Radar Chart) หรือบางครั้งเรียกว่า "แผนภูมิใยแมงมุม" (Spider Chart)

เปรียบเทียบเครื่องมือประเมินความแข็งแกร่งของรหัสผ่านทั้ง 4 เครื่องมือ ได้แก่ UIC (สีแดง), PM (สีเขียว), PW (สีน้ำเงิน) และ PH (สีชมพู) บนแผนภูมิเรดาร์ตามประสิทธิภาพตามเกณฑ์รหัสผ่าน 15 ข้อ ดังนี้

1. รูปร่างและความครอบคลุม รูปร่างของแผนภูมิเรดาร์ของเครื่องมือแต่ละรายการจะให้ข้อมูลเชิงลึกว่าเครื่องมือเหล่านี้ให้คะแนนรหัสผ่านประเภทต่าง ๆ อย่างสม่ำเสมอเพียงใด รูปร่างวงกลมที่มากขึ้นบ่งบอกถึงความสม่ำเสมอในการให้คะแนนของรหัสผ่านประเภทต่าง ๆ ในขณะที่รูปร่างที่ผิดปกติบ่งบอกถึงความแปรปรวน ขนาดของพื้นที่ที่ครอบคลุมโดยแผนภูมิเรดาร์ของเครื่องมือแต่ละชิ้นแสดงให้เห็นถึงความผ่อนปรนหรือความเข้มงวดโดยรวม

2. การสังเกตเฉพาะเครื่องมือ

2.1 UIC หากพล็อตของ UIC ขยายไปสู่เกณฑ์ที่อ่อนแอกว่า (เช่น 8Num, 8Char) ก็อาจจะค่อนข้างต่ำหรือคงไว้ในกรณีเหล่านี้ ในทางกลับกัน พื้นที่ที่เล็กกว่าบนเกณฑ์ที่ซับซ้อนมากขึ้นบ่งชี้ถึงการให้คะแนนที่เข้มงวดมากขึ้น

2.2 PM อาจแสดงจุดแข็งหรือจุดอ่อนในรหัสผ่านประเภทใดประเภทหนึ่ง ขึ้นอยู่กับว่าแผนผังนั้นขยายออกไปในเรดาร์อย่างไร ตัวอย่างเช่น การครอบคลุมรหัสผ่านที่ซับซ้อนมากขึ้น (เช่น 12NumCharCapSpe) จะแนะนำว่ารหัสผ่านมีความผ่อนปรนมากกว่าหรือมองว่ารหัสผ่านเหล่านี้แข็งแกร่งกว่า

2.3 PW แผนภาพเรดาร์ของ PW อาจบ่งบอกถึงแนวทางที่สมดุล หากยังคงรักษารูปร่างที่สอดคล้องกันตามเกณฑ์ต่าง ๆ การเบี่ยงเบนใด ๆ อาจเน้นบริเวณที่มีความเข้มงวดไม่มากก็น้อย

2.4 PH อาจโดดเด่นหากโครงเรื่องแสดงความแตกต่างที่มีนัยสำคัญในด้านความครอบคลุมเมื่อเปรียบเทียบกับเครื่องมืออื่นๆ ซึ่งบ่งบอกถึงแนวโน้มการให้คะแนนที่ไม่ซ้ำใคร

3. การทับซ้อนกันและความแตกต่าง พื้นที่ที่แปลงทับซ้อนกันบ่งบอกถึงการให้คะแนนที่ใกล้เคียงกันในเครื่องมือต่าง ๆ ในขณะที่พื้นที่ที่มีการทับซ้อนกันเพียงเล็กน้อยหรือไม่มีการทับซ้อนบ่งบอกถึงความคลาดเคลื่อน เครื่องมือที่เห็นด้วยกับรหัสผ่านบางประเภทจะมีแผนเรดาร์ที่ทับซ้อนกันในส่วนเหล่านั้น

4. ค่าผิดปกติและค่าผิดปกติ หากแผนภูมิเรดาร์ของเครื่องมือเบี่ยงเบนไปจากส่วนอื่น ๆ ในพื้นที่เฉพาะอย่างมาก ก็อาจมีค่าผิดปกติในการจัดอันดับรหัสผ่านประเภทเหล่านั้น ซึ่งอาจบ่งชี้ถึงแนวทางการให้คะแนนขั้นสูงหรือแบบอนุรักษ์นิยม

อภิปรายผลการวิจัย

ความแม่นยำในการประเมินความแข็งแกร่งของรหัสผ่านการศึกษาผลลัพธ์ที่เกี่ยวข้องกับความแม่นยำในการประเมินความแข็งแกร่งของรหัสผ่านได้เปิดเผยข้อมูลที่น่าสนใจเกี่ยวกับประสิทธิภาพของเครื่องมือที่ใช้ในการวิเคราะห์รหัสผ่านต่าง ๆ ผลการวิจัยชี้ให้เห็นว่าเครื่องมือบางประเภทมีความสามารถในการระบุรหัสผ่านที่ไม่มีความปลอดภัยได้อย่างแม่นยำสูง ในขณะที่เครื่องมืออื่น ๆ มีความสามารถที่ดีกว่าในการตรวจจับรหัสผ่านที่มีความซับซ้อนและปลอดภัยมากขึ้น

การอภิปรายเกี่ยวกับความแปรผันของระดับความแม่นยำนี้สามารถเชื่อมโยงกับอัลกอริธึมและเทคนิคการวิเคราะห์พฤติกรรมที่แตกต่างกันซึ่งถูกนำมาใช้โดยเครื่องมือแต่ละประเภท ตัวอย่างเช่น เครื่องมือที่ใช้เทคนิคการเรียนรู้ของเครื่อง (Machine Learning) อาจมีความสามารถในการปรับปรุงการตรวจสอบรหัสผ่านที่มีความซับซ้อนได้ดีกว่า ในขณะที่เครื่องมือที่ใช้วิธีการแบบดั้งเดิมอาจไม่สามารถปรับตัวได้ตามความเปลี่ยนแปลงของพฤติกรรมผู้ใช้สิ่งนี้ชี้ให้เห็นถึงความจำเป็นในการสร้างแนวทางที่เป็นมาตรฐานมากขึ้นในการประเมินความแข็งแกร่งของรหัสผ่าน เพื่อให้สามารถเปรียบเทียบประสิทธิภาพของเครื่องมือต่าง ๆ ได้อย่างมีประสิทธิภาพและเชื่อถือได้ การพัฒนามาตรฐานที่ชัดเจนจะช่วยให้ผู้ใช้สามารถเลือกเครื่องมือที่

ดีที่สุดสำหรับการป้องกันข้อมูลส่วนบุคคลของตน และยังช่วยในการพัฒนานวัตกรรมใหม่ๆ ในการรักษาความปลอดภัยของรหัสผ่านในอนาคตได้อีกด้วย

ผลกระทบของการวิจัย

การค้นพบนี้มีผลกระทบอย่างมีนัยสำคัญต่อทั้งผู้ใช้และนักพัฒนาเครื่องมือวิเคราะห์ความแข็งแกร่งของรหัสผ่าน โดยเฉพาะอย่างยิ่งในบริบทของความปลอดภัยออนไลน์ที่มีความสำคัญยิ่งในยุคดิจิทัลปัจจุบัน สำหรับผู้ใช้ผลลัพธ์ที่ได้จากการศึกษาภาคนิพนธ์นี้จะมอบข้อมูลเชิงลึกที่มีค่าเกี่ยวกับความน่าเชื่อถือของเครื่องมือที่ใช้ในการประเมินความแข็งแกร่งของรหัสผ่าน โดยผู้ใช้จะสามารถเลือกเครื่องมือที่ให้การประเมินที่ถูกต้องและเชื่อถือได้มากที่สุด ซึ่งจะช่วยเพิ่มความมั่นใจในการเลือกใช้รหัสผ่านที่ปลอดภัย และลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ในขณะเดียวกัน สำหรับนักพัฒนา การค้นพบนี้ยังได้เน้นย้ำถึงประเด็นสำคัญที่ต้องมีการปรับปรุงในด้านการออกแบบและฟังก์ชันการทำงานของเครื่องมือวิเคราะห์เหล่านี้ โดยการเข้าใจถึงข้อบกพร่องและจุดอ่อนที่มีอยู่ในเครื่องมือปัจจุบัน จะช่วยให้สามารถพัฒนาเครื่องมือที่มีประสิทธิภาพมากยิ่งขึ้น และตอบสนองต่อความต้องการของผู้ใช้ได้อย่างเหมาะสม

ผลการศึกษาวิจัยนี้ไม่เพียงแต่ช่วยเสริมสร้างความรู้และความเข้าใจในด้านความปลอดภัยของรหัสผ่าน แต่ยังเป็นแรงผลักดันในการพัฒนาเครื่องมือที่มีคุณภาพสูงขึ้น ซึ่งจะนำไปสู่การสร้างสภาพแวดล้อมออนไลน์ที่ปลอดภัยยิ่งขึ้นสำหรับทุกคน

ข้อเสนอแนะ

จากการวิเคราะห์และประเมินผลที่ได้จากการศึกษาในครั้งนี้ มีคำแนะนำที่สำคัญเพื่อ ปรับปรุงความแม่นยำ ความสม่ำเสมอ และการใช้งานของเครื่องมือวิเคราะห์ความแข็งแกร่งของรหัสผ่าน ซึ่งคำแนะนำเหล่านี้ผู้วิจัยได้มองเห็นถึงวัตถุประสงค์เพื่อเป็นแนวทางในการพัฒนาศักยภาพของเครื่องมือในอนาคตในสาขานี้ โดยสามารถแบ่งข้อเสนอแนะออกมาได้ 4 ข้อดังนี้

1. การปรับปรุงอัลกอริธึมการวิเคราะห์ที่ใช้ในการวิเคราะห์ความแข็งแกร่งของรหัสผ่านให้มีความทันสมัยและสามารถตอบสนองต่อรูปแบบการโจมตีใหม่ ๆ ที่เกิดขึ้น ซึ่งจะช่วยเพิ่มความแม่นยำในการประเมินความปลอดภัยของรหัสผ่านได้ดียิ่งขึ้น
2. การเพิ่มฟีเจอร์การใช้งานควรพิจารณาเพิ่มฟีเจอร์ใหม่ ๆ ที่สามารถช่วยให้ผู้ใช้เข้าใจ ความแข็งแกร่งของรหัสผ่านได้ดียิ่งขึ้น เช่น การให้คำแนะนำในการสร้างรหัสผ่านที่ปลอดภัย หรือการเสนอวิธีการจัดการรหัสผ่านที่มีประสิทธิภาพ
3. การทดสอบและประเมินผลอย่างต่อเนื่องควรมีการทดสอบและประเมินผลเครื่องมืออย่างต่อเนื่องเพื่อให้แน่ใจว่าเครื่องมือยังคงมีความแม่นยำและสามารถใช้งานได้ดีในสภาพแวดล้อมที่เปลี่ยนแปลงไป
4. การสร้างความตระหนักรับรู้ในผู้ใช้เกี่ยวกับความสำคัญของการใช้รหัสผ่านที่แข็งแกร่ง และวิธีการใช้เครื่องมือวิเคราะห์เพื่อเสริมสร้างความปลอดภัยให้กับข้อมูลส่วนบุคคล คำแนะนำเหล่านี้ไม่เพียงแต่จะช่วยพัฒนาเครื่องมือวิเคราะห์ความแข็งแกร่งของรหัสผ่านให้มีประสิทธิภาพมากยิ่งขึ้น แต่ยังสามารถส่งเสริมความปลอดภัยในโลกดิจิทัลที่มีการเปลี่ยนแปลงอย่างรวดเร็วได้อีกด้วย

ข้อจำกัดของการศึกษาวิจัย

1. เสริมสร้างความเข้าใจในพฤติกรรมการสร้างรหัสผ่านการศึกษานี้ช่วยวิเคราะห์พฤติกรรมของผู้ใช้ในการสร้างรหัสผ่าน ทำให้เข้าใจแนวโน้มและรูปแบบที่ผู้ใช้มักเลือกใช้ ซึ่งเป็นข้อมูลสำคัญในการพัฒนาแนวทางการรักษาความปลอดภัยที่มีประสิทธิภาพ

2. เปรียบเทียบประสิทธิภาพของเครื่องมือวิเคราะห์การศึกษาเปรียบเทียบเครื่องมือวิเคราะห์ความแข็งแกร่งของรหัสผ่านต่าง ๆ ช่วยให้เห็นข้อดีและข้อจำกัดของแต่ละเครื่องมือ นำไปสู่การเลือกใช้และพัฒนาเครื่องมือที่เหมาะสมยิ่งขึ้น

3. พื้นฐานสำหรับการพัฒนาเครื่องมือใหม่ผลการศึกษาสามารถเป็นแนวทางในการพัฒนาเครื่องมือวิเคราะห์รหัสผ่านรุ่นใหม่ที่มีความแม่นยำและครอบคลุมมากขึ้น

การศึกษานี้จึงมีคุณค่าทั้งในแง่ของการเพิ่มพูนความรู้ทางวิชาการและการนำไปประยุกต์ใช้ในทางปฏิบัติ เพื่อยกระดับความปลอดภัยของข้อมูลส่วนบุคคลและองค์กรในยุคดิจิทัล

ทิศทางการวิจัยในอนาคต

จากผลการศึกษาและข้อจำกัดที่พบ ทิศทางการวิจัยในอนาคตควรมุ่งเน้นการพัฒนาสี่ด้านหลัก ได้แก่ ด้านเทคนิค เช่น การพัฒนาเกณฑ์มาตรฐานสำหรับการประเมินเครื่องมือ การศึกษาและพัฒนาอัลกอริธึมใหม่ที่มีประสิทธิภาพสูงขึ้น และการประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์และ Machine Learning ในการวิเคราะห์และคาดการณ์ภัยคุกคามรูปแบบใหม่ ด้านพฤติกรรมผู้ใช้ที่มุ่งศึกษาการสร้างและใช้รหัสผ่านในสถานการณ์จริง รวมถึงผลกระทบของเครื่องมือวิเคราะห์ต่อพฤติกรรมการเลือกใช้รหัสผ่าน

นอกจากนี้ ควรขยายขอบเขตการวิจัยไปสู่การศึกษาเปรียบเทียบระหว่างวัฒนธรรม เพื่อพัฒนาเครื่องมือที่สามารถปรับตัวให้เข้ากับความหลากหลายทางภาษาและวัฒนธรรม รวมถึงการบูรณาการกับระบบความปลอดภัยอื่นๆ เช่น การยืนยันตัวตนแบบหลายปัจจัย ตลอดจนการวิจัยด้านการให้ความรู้และสร้างความตระหนักแก่ผู้ใช้ เพื่อพัฒนาวิธีการถ่ายทอดความรู้ที่มีประสิทธิภาพและศึกษาผลกระทบระยะยาวต่อพฤติกรรมการใช้รหัสผ่าน ทั้งหมดนี้จะช่วยยกระดับความปลอดภัยของการใช้รหัสผ่านในยุคดิจิทัลให้มีประสิทธิภาพมากยิ่งขึ้น

ผลการวิจัยที่นำไปใช้ประโยชน์

1. ด้านวิชาการ เป็นแหล่งอ้างอิงสำหรับการศึกษาและวิจัยเกี่ยวกับการประเมินความปลอดภัยของรหัสผ่านพัฒนาเกณฑ์มาตรฐานในการประเมินเครื่องมือวิเคราะห์ความแข็งแกร่งของรหัสผ่าน สร้างองค์ความรู้ใหม่ด้านความปลอดภัยทางไซเบอร์

2. ด้านการพัฒนาระบบ ช่วยในการเลือกใช้เครื่องมือที่เหมาะสมสำหรับการประเมินความแข็งแกร่งของรหัสผ่าน นำไปปรับปรุงและพัฒนาระบบรักษาความปลอดภัยให้มีประสิทธิภาพมากขึ้นใช้เป็นแนวทางในการพัฒนาเครื่องมือประเมินรหัสผ่านรุ่นใหม่

3. ด้านการนำไปใช้งานจริง องค์กรสามารถนำผลการวิจัยไปประยุกต์ใช้ในการกำหนดนโยบายด้านความปลอดภัย ผู้ใช้งานทั่วไปได้รับความรู้ในการสร้างรหัสผ่านที่ปลอดภัย สถาบันการศึกษาสามารถนำไปใช้ในการเรียนการสอนด้านความปลอดภัยทางไซเบอร์

สรุปผลการศึกษา

ผลการศึกษาเกี่ยวกับ การวิเคราะห์เปรียบเทียบประสิทธิภาพของเครื่องมือประเมินความแข็งแกร่งของรหัสผ่านสำหรับระบบรักษาความปลอดภัยทางไซเบอร์ โดยมีประเด็นสำคัญดังนี้การเปรียบเทียบเครื่องมือศึกษาเครื่องมือ 4 ชนิด ได้แก่ UIC, PM, PW และ PH แต่ละเครื่องมือมีจุดแข็งและข้อจำกัดที่แตกต่างกันพบความไม่สอดคล้องในการประเมินระหว่างเครื่องมือ โดยเฉพาะในรหัสผ่านที่มีความซับซ้อนปานกลางประสิทธิภาพของเครื่องมือ PH มีความเข้มงวดในการประเมินมากที่สุด PW มีความสม่ำเสมอในการประเมินสูงที่สุด UIC และ PM มีความสมดุลระหว่างความเข้มงวดและการใช้งานจริงผลกระทบของความยาวและความซับซ้อนของรหัสผ่าน รหัสผ่านที่ยาวขึ้นและมีความซับซ้อนมากขึ้นได้รับการประเมินว่าแข็งแกร่งกว่าอย่างมีนัยสำคัญการผสมผสานตัวอักษร ตัวเลข และอักขระพิเศษช่วยเพิ่มความแข็งแกร่งของรหัสผ่านข้อจำกัดของการศึกษาการศึกษาจำกัดเฉพาะเครื่องมือบนเว็บไซต์ชุดข้อมูลทดสอบอาจไม่ครอบคลุมทุกรูปแบบรหัสผ่านที่เป็นไปได้ไม่สามารถเข้าถึงอัลกอริธึมภายในของเครื่องมือได้ทิศทางการวิจัยในอนาคต พัฒนาเกณฑ์มาตรฐานสำหรับการประเมินเครื่องมือศึกษาการใช้ AI และ Machine Learning ในการวิเคราะห์รหัสผ่านวิจัยเกี่ยวกับพฤติกรรมผู้ใช้และการให้ความรู้ด้าน ความปลอดภัยผลกระทบต่อความปลอดภัยทางไซเบอร์ เน้นย้ำความสำคัญของการใช้รหัสผ่านที่แข็งแกร่งชี้ให้เห็นถึงความจำเป็นในการพัฒนาเครื่องมือที่มีประสิทธิภาพและน่าเชื่อถือสนับสนุนการสร้างความตระหนักรู้เกี่ยวกับความปลอดภัยของรหัสผ่านข้อเสนอแนะใช้เครื่องมือหลายชนิดร่วมกันเพื่อการประเมินที่ครอบคลุมพัฒนาเครื่องมือให้มีความเป็นมิตรต่อผู้ใช้มากขึ้นส่งเสริมการให้ความรู้แก่ผู้ใช้เกี่ยวกับการสร้างรหัสผ่านที่ปลอดภัย

โดยสรุป การศึกษานี้ให้ข้อมูลเชิงลึกเกี่ยวกับสถานะปัจจุบันของเครื่องมือวิเคราะห์ความแข็งแกร่งของรหัสผ่านชี้ให้เห็นถึงความสำคัญของการพัฒนาและใช้งานเครื่องมือเหล่านี้อย่างมีประสิทธิภาพ เพื่อเสริมสร้างความปลอดภัยในโลกดิจิทัล พร้อมทั้งเสนอแนะแนวทางสำหรับการวิจัยและพัฒนาในอนาคตเพื่อยกระดับความปลอดภัยของรหัสผ่านและความปลอดภัยทางไซเบอร์โดยรวม

เอกสารอ้างอิง

Adams, A., & Sasse, M. A. (1999). Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures. Communications of the ACM, 42(12), 41-46.

Burnett, Mark. (2013). More Top Worst Passwords. Retrieved February 25, 2013, from https://xato.net/passwords/more-top-worst-passwords/#more-269

Computer History Museum. (2014). "Moore's Law" predicts the future of integrated circuits. Retrieved February 25, 2014, from http://www.computerhistory.org/semiconductor/timeline/1965-Moore.html

Dell'Amico, M., Michiardi, P., & Roudier, Y. (2010). Password Strength: An Empirical Analysis. 2010 Proceedings IEEE INFOCOM, 1-9. https://doi.org/10.48550/arXiv.0907.3402

Emam, K. E., Moreau, K., & Jonker, E. (2011). How strong are passwords used to protect personal health information in clinical trials?. Journal of Medical Internet Research, 13(1), e18. https://doi.org/10.2196/jmir.1335

Furnell, S. (2019). Password meters: inaccurate advice offered inconsistently?. Computer Fraud and Security, 2019(11), 6-14. https://doi.org/10.1016/s1361-3723(19)30116-2

Güven, E. Y., Boyacı, A., & Aydın, M. A. (2022). A novel password policy focusing on altering user password selection habits: a statistical analysis on breached data. Computers and Security, 113, 102560. https://doi.org/10.1016/j.cose.2021.102560

Harley, David. (2013). Passwords and PINs: The Worst Choices. Retrieved February 25, 2013, from http://www.welivesecurity.com/2012/06/07/passwords-and-pins-the-worst-choices/

Hatfield, J. M. (2018). Social engineering in cybersecurity: the evolution of a concept. Computers and Security, 73, 102-113. https://doi.org/10.1016/j.cose.2017.10.008

Intel Corporation. (2013). Microprocessor Quick Reference Guide. Retrieved February 25, 2013, from http://www.intel.com/pressroom/kits/quickreffam.htm

Juozapavičius, A., Brilingaitė, A., Bukauskas, L., & Lugo, R. G. (2022). Age and gender impact on password hygiene. Applied Sciences, 12(2), 894. https://doi.org/10.3390/app12020894

Kanta, A., Coisel, I., & Scanlon, M. (2023). Harder, better, faster, stronger: optimising the performance of context-based password cracking dictionaries. Forensic Science International: Digital Investigation, 44, 301507. https://doi.org/10.1016/j.fsidi.2023.301507

Kennison, S. M., Jones, I. T., Spooner, V. H., & Chan-Tin, D. E. (2021). Who creates strong passwords when nudging fails. Computers in Human Behavior Reports, 4, 100132. https://doi.org/10.1016/j.chbr.2021.100132

Moore, G. E. (2006). Cramming more components onto integrated circuits. IEEE Solid-State Circuits Society Newsletter, 11(3), 33-35. https://doi.org/10.1109/N-SSC.2006.4785860

National Bureau of Standards. (1985). Federal Information Processing Standards Publication: password usage. Gaithersburg : National Bureau of Standards

National Institute of Standards and Technology. (2023). National Institute of Standards and Technology Environmental Scan 2023: Societal and Technology Landscape to Inform Science and Technology Research. [Online]. Available: https://www.nist.gov/publications/national-institute-standards-and-technology-environmental-scan-2023-societal-and

NIST Special Publication. (2024). Digital Identity Guidelines: Authentication and Lifecycle Management. [Online]. Available: https://www.nist.gov/publications/digital-identity-guidelines-authentication-and-lifecycle-management

SANS Password Protection Policy. (2022). SANS. [Online]. Available : https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltf5d5757503e36442/636f1a316bafb12e165da155/Password_Protection_Policy.pdf

Schneier, B. (2007, January). Choosing secure passwords. Schneier on Security. Retrieved from http://www.schneier.com/blog/archives/2007/01/choosing_secure.html

Sobrado, L., & Birget, J.-C. (2002). Graphical passwords. The Rutger Scholar, 4. Retrieved from https://rutgersscholar.libraries.rutgers.edu/index.php/scholar/article/view/60

Tanni, T. I., Taharat, T., Parvez, M., Rumee, S. T. A., & Zaber, M. (2022). Is my password strong enough?: a study on user perception in the developing world. EAI Endorsed Transactions on Creative Technologies, 9(30), 173452. https://doi.org/10.4108/eai.11-2-2022.173452

Tao, H., & Adams, C. (2006). Pass-Go: A proposal to improve the usability of graphical passwords. International Journal of Network Security, 7(2), 273-292.

Weir, M., Aggarwal, S., Collins, M., & Stern, H. (2010). Testing metrics for password creation policies by attacking large sets of revealed passwords. ACM. Retrieved from http://goo.gl/wqcX

Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., & Memon, N. (2005). Authentication using graphical passwords. Proceedings of the 2005 Symposium on Usable Privacy and Security - SOUPS '05, 1-12. https://doi.org/10.1145/1073001.1073002

Wikipedia. (2013, February 25). Password strength. In Wikipedia, The Free Encyclopedia. Retrieved February 25, 2013, from http://en.wikipedia.org/wiki/Password_strength

Wu, T. D. (1999). A real-world analysis of Kerberos password security. In Proceedings of the Network and Distributed System Security Symposium (NDSS). https://www.ndss-symposium.org/wp-content/uploads/2017/09/A-Real-World-Abstract-Analysis-of-Kerberos-Password-Security-Thomas-Wu.pdf

Zhou, E., Peng, Y., Shao, G., Deng, F., Miao, Y., & Fan, W. (2024). Password cracking using chunk similarity. Future Generation Computer Systems, 150, 380-394. https://doi.org/10.1016/j.future.2023.09.013