ระบบรหัสผ่านแบบใช้ครั้งเดียวที่เสริมสร้างความมั่นคง

สมนึก พ่วงพรพิทักษ์[1*]

บทคัดย่อ

ในระบบพิสูจน์ตัวจริงแบบพหุปัจจัย รหัสผ่านใช้ครั้งเดียวหรือที่เรียกว่า โอทีพี เป็นส่วนประกอบที่สำคัญและถูกใช้งานอย่างกว้างขวางที่สุดอันหนึ่ง โดยทั่วไปมันจะถูกใช้เป็นปัจจัยที่สองในการพิสูจน์ตัวจริงเพื่อป้องกันระบบในกรณีที่รหัสผ่าน (ซึ่งเป็นปัจจัยการพิสูจน์ตัวจริงแรก) เกิดมีการรั่วไหล ในงานวิจัยนี้ได้วิเคราะห์ปัญหาด้านความมั่นคงของระบบโอทีพีที่มีในปัจจุบัน และได้ออกแบบและพัฒนาต้นแบบของระบบโอทีพีใหม่ โดยเสริมสร้างความมั่นคง ซึ่งระบบโอทีพีที่เสนอประกอบด้วย เว็บเซอร์วิสโอทีพี และโปรแกรมโอทีพีบนโทรศัพท์มือถือ โดยมีการเสริมสร้างความมั่นคงดังต่อไปนี้ (1) การแก้ไขอัลกอริทึมรหัสผ่านใช้ครั้งเดียวที่มีฐานจากเวลา โดยใช้ SHA-256 แทน SHA-1 (2) การปรับปรุงโหมดการแสดงผลของโอทีพี: num6, mix6base40, th6base42, th6base60 (3) คุณสมบัติการล็อกโอทีพีเข้ากับฮาร์ดแวร์ของโทรศัพท์มือถือ, (4) การตรวจสอบหมายเลขที่อยู่ไอพีที่เรียกใช้ระบบเว็บเซอร์วิสโอทีพี นอกจากนี้ งานวิจัยนี้ได้ทำการทดลองกับระบบต้นแบบที่พัฒนาขึ้น เพื่อประเมินระบบโอทีพีที่ได้ออกแบบ ผลการทดลองได้แสดงให้เห็นถึงประสิทธิภาพและความมั่นคงของระบบ

คำสำคัญ : การพิสูจน์ตัวจริงแบบพหุปัจจัย; รหัสผ่านใช้ครั้งเดียวจากฐานเวลา; ระบบรหัสผ่านใช้ครั้งเดียว

---

[1] Information Security and Advanced Network (ISAN) research Group, Department of Computer Science, Faculty of Informatics, Mahasarakham University

*ผู้แต่ง, อีเมล: somnuk.p@msu.ac.th