ระบบซอฟท์แวร์แอ๊บพริเคชั่นที่ทำงานผ่านอินเทอร์เน็ตได้ถูกพัฒนาขึ้นและนำมาใช้งานอย่างแพร่หลาย ซึ่งการใช้อย่างแพร่หลายดังกล่าว เปิดช่องทางให้ผู้ที่ไม่หวังดีต่อระบบ สามารถทำการโจมตีระบบเพื่อทำการดูข้อมูลที่เป็นความลับของระบบ หรือเปลี่ยนแปลงข้อมูลดังกล่าว หรือเพื่อก่อกวนทำให้ระบบไม่สามารถทำงานได้ตามปกติ งานวิจัยชิ้นนี้มีจุดประสงค์ที่จะศึกษาแนวทางการนำวิธีการแบบฟอร์มอลมาใช้ในการวิเคราะห์การรักษาความมั่นคงปลอดภัยของโพรโตคอลที่ใช้เทคนิคการเข้ารหัสข้อมูล และของระบบเครือข่ายไฟร์วอลล์ ผลที่ได้จากการศึกษาในโครงการนี้ คือ ได้ระเบียบวิธีการแบบฟอร์มอลล์ในการวิเคราะห์ความปลอดภัยของโพรโตคอลที่ใช้เทคนิคการเข้ารหัสข้อมูล ที่มีเป็นประโยชน์ในแนวทางการใช้สอยและมีประสิทธิภาพสูงขึ้น ซึ่งทำให้ผู้วิจัยได้ค้นพบการโจมตีใหม่ ในโพรโตคอลการแลกเปลี่ยนกุญแจแบบที่มียืนยันตัวตนที่แท้จริงเพื่อการใช้งานในการสื่อสารแบบเคลื่อนที่ และโพรโตคอลสำหรับการเซ็นต์สัญญาข้อมูลระหว่างสองบุคคล นอกจากนั้นโครงการนี้ยังได้รับผลคือ ได้แบบจำลองและวิธีการแบบฟอร์มอลล์ในการวิเคราะห์ความปลอดภัยในระบบเครือข่ายไฟร์วอลล์ ที่มีประสิทธิภาพสูงขึ้น และซอฟท์แวร์ต้นแบบเบื้องต้นที่สามารถใช้ในการประมวลผลการวิเคราะห์ความปลอดภัยของกฎไฟร์วอลล์

220508

Nowadays, many internet-based applications have been developed and used widely. However, the wide adoption of such internet-based applications opens up many opportunities to malicious parties to attack the systems. In particular, attackers can access and modify sensitive information transmitted between the systems. Also, attackers can interfere with systems so that the systems become unavailable for legitimate users. This project aims to study a formal method to analyze cryptographic protocols and the security of network firewalls. As a result of this project, we have obtained an improved formal method for the analysis of cryptographic protocols and network firewalls. In particular, we propose a new practical methodology for analyzing cryptographic protocols. By using our improved method, we have discovered new attacks on two protocols : TMN's authenticated key exchange protocol for mobile communication system and Micali's fair contract signing protocol. In addition, we obtain a more efficient method for the analysis of firewalls and a software prototype of our method.