บทคัดย่อ

รหัสโครงการ PDF/20/2542

ชื่อโครงการ วิธีการรวมแบบตรรกะศาสตร์ สำหรับนโยบายการรักษาความปลอดภัยในคอมพิวเตอร์

ชื่อนักวิจัย ผศ. ดร. ยงยุทธ เพิ่มพูนธนลาภ

ห้องปฏิบัติการวิจัย Logic และ Security

ภาควิชาวิศวกรรมคอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้า ธนบุรี

Email Address : yongyuth@cpe.eng.kmutt.ac.th, ypber@yahoo.com

ระยะเวลาโครงการ 2 ปี

งานวิจัยชิ้นนี้มีจุดประสงค์ในการพัฒนาวิธีการแบบนัยนิยมที่สามารถนำมาใช้วิเคราะห์ระบบการรักษาความปลอดภัยของข้อมูลสารสนเทศในผลิตภัณฑ์ที่ใช้งานจริง โดยเฉพาะอย่างยิ่งผู้วิจัยได้พัฒนาวิธีการแบบนัยนิยมสำหรับการควบคุมการเข้าถึงข้อมูลสารสนเทศในระบบปฏิบัติการ ระบบไฟร์วอลล์ และโพรโตคอลสำหรับการชำระเงินอีเล็กโทรนิกส์ซึ่งใช้ในระบบพาณิชย์อีเล็กโทรนิกส์ ซึ่งวิธีการแบบนัยนิยมที่พัฒนาขึ้นประกอบด้วย แบบจำลองซึ่งสามารถอธิบายการทำงานของระบบดังกล่าวได้ชัดเจนไม่คลุมเคลือ และการพิสูจน์ตรวจสอบความปลอดภัยในผลิตภัณฑ์ดังกล่าว

ซอฟท์แวร์ต้นแบบได้ถูกพัฒนาขึ้นและได้ถูกนำไปใช้งานในกรณีศึกษา ซึ่งจากการทำการทดลองในกรณีศึกษาพบว่า วิธีการแบบนัยนิยมที่ได้ถูกพัฒนาขึ้นสามารถอธิบายการทำงานของระบบการรักษาความปลอดภัยของข้อมูลได้ชัดเจน ไม่คลุมเครือ ส่งผลให้นำมาสู่ความเข้าใจในการทำงานของระบบและการใช้งานของระบบที่ดีขึ้น นอกจากนี้วิธีการที่ได้ถูกพัฒนาขึ้นสามารถนำมาใช้ในการวิเคราะห์การใช้งานของระบบโดยเน้นประโยชน์ใช้สอย โดยเฉพาะอย่างยิ่งการวิเคราะห์ความถูกต้องและความปลอดภัยขั้นพื้นฐานของการใช้งานของระบบได้ดี

สำหรับงานวิจัยในอนาคต ผู้วิจัยคาดว่าจะทำการศึกษาวิธีการวิเคราะห์การบุกรุกในระบบอินเทอร์เน็ตและวิธีการในการวิเคราะห์และช่วยสร้างโพรโตคอลที่มีความปลอดภัยสำหรับรัฐบาลอีเล็กโทรนิกส์

Keywords : Formal Method for Computer Security, Access Control, Firewalls, Cryptographic Protocols

Abstract

Project Code : PDF/20/2542

Project Title : A Unified Logical Methodology for Security Policy

Investigator : Assistant Professor Dr. Yongyuth Permpoontanalarp

Logic and Security Laboratory, Department of Computer Engineering

King Mongkut's University of Technology Thonburi

Email Address : yongyuth@cpe.eng.kmutt.ac.th, ypber@yahoo.com

Project Period : 2 years

This research aims to develop a formal methodology for analyzing the security of information security systems which are currently in use nowadays. In particular, we have developed formal methodology for access control in operating systems, network firewalls and electronic payment protocols. The formal methodology developed consists of formal specification which describes system behavior unambiguously and formal verification that can analyze the security of those systems.

A software prototype is developed and is applied to case studies. Experimental results obtained from the case studies show that our methodology can explain system behavior precisely and unambiguously. This provides a better understanding on how the systems work and how to use them correctly. Furthermore, our verification method offers practical analysis on the correctness and the security of the systems. In particular, important properties and attacks can be analyzed.

As a future work, we aim to develop further our method for analyzing attacks in Internet and cryptographic protocols for electronic government systems.

Keywords : Formal Method for Computer Security, Access Control, Firewalls, Cryptographic Protocols