MODELING AND ANALYSIS OF TWO-FACTOR AUTHENTICATION PROTOCOL FOR USB DIGITAL EVIDENCE ACQUISITION DEVICES

SIRIPOOM LAPTIKULTHAM 5438250 EGCO/M

M.Eng.(COMPUTER ENGINEERING)

THESIS ADVISORY COMMITTEE : SURATOSE TRITILANUNT, Ph.D., KONGLIT HUNCHANGSITH, Ph.D., NOPPADOL WANICHWORANANT, Ph.D.

ABSTRACT

Currently, there are several problems regarding the usage of a USB storage device. One major concern is in the problem of lacking authorization and in the authentication of software and data stored on that storage devices. Many research papers offer high-levels of security by adding *Two-factor authentication* to USB devices and use additional equipment such as Smartphones, or Token-Based devices, to generate this parameter. These devices help the user to create a second parameter of authentication such as OTP (One-time password) or PIN (Personal identification number). However, these protocols are still inappropriate in terms of adopting into devices for digital forensic applications.

This thesis reviews some related literatures of authentication protocols. We developed the protocol for USB authentication, which was considered to focus on light-weight computation and require the minimum number of exchanged messages between 2 entities. Then the proposed model was analyzed by using a Coloured Petri Net, which is the Formal method tool for modeling and verifying the communication system. We also created two difference scenarios of attacker in the model in order to show that our purposed protocol had been proven secure. Finally, the prototype software of the proposed protocol is implemented thus validating the protocol functionality and workflow.

KEY WORDS: TWO-FACTOR AUTHENTICATION / COLOURED PETRI NET MODEL / CPN TOOLS / USB DATA STORAGE DEVICE

71 pages

การสร้างแบบจำลองและการวิเคราะห์โปรโตคอลยืนยันตัวตนแบบสองระดับสำหรับอุปกรณ์เก็บข้อมูลหลักฐานทางดิจิทัลแบบ USB

MODELING AND ANALYSIS OF TWO-FACTOR AUTHENTICATION PROTOCOL FOR USB DIGITAL EVIDENCE ACQUISITION DEVICES

ศิริภูมิ ลัพธิกุลธรรม 5438250 EGCO/M

วศ.ม.(วิศวกรรมคอมพิวเตอร์)

คณะกรรมการที่ปรึกษาสารนิพนธ์: สุรทศ ไตรติลานันท์, Ph.D.,คงฤทธิ์ หันจางสิทธิ์, Ph.D.,นภดล วณิชวรนันท์, Ph.D.

บทคัดย่อ

ปัจจุบันมีปัญหาหลายประการที่เกี่ยวกับการใช้งานอุปกรณ์เก็บข้อมูล USB ซึ่งหนึ่งในนั้นคือการที่ปราศจากการอนุญาตให้ใช้งานและการยืนยันตัวตนของซอฟแวร์และข้อมูลที่ถูกเก็บไว้ภายในอุปกรณ์นั้นๆ มีงานวิจัยหลายฉบับที่นำเสนอระบบความปลอดภัยที่สูงขึ้นโดยการใช้ *การยืนยันตัวตนโดยใช้ 2 ปัจจัย* กับอุปกรณ์หน่วยความจำแบบต่อพ่วงชนิด USB โดยมีอุปกรณ์เสริมอย่างเช่น สมาร์ทโฟน หรือ อุปกรณ์ที่เป็น Token-based ซึ่งสามารถสร้างสถานะสำหรับการยืนยันตัวตนขั้นที่สองได้ เช่นการใช้รหัสผ่านแบบใช้ครั้งเดียวหรือรหัสยืนยันส่วนบุคคล แต่โปรโตคอลเหล่านี้ยังไม่เหมาะสมที่จะนำมาใช้กับอุปกรณ์ที่พัฒนาขึ้นมาเพื่อใช้สำหรับงานทางด้านนิติวิทยาดิจิทัล

งานวิจัยฉบับนี้ผู้วิจัยได้ศึกษางานวิจัยอื่นที่เกี่ยวข้องกับโปรโตคอลการยืนยันตัวตนและได้ทำการพัฒนาโปรโตคอลการยืนยันตัวตนสำหรับอุปกรณ์เก็บข้อมูลชนิด USB โดยเน้นไปที่การประมวลผลต่ำและจำนวนขั้นตอนในการแลกเปลี่ยนข้อมูลน้อย โดยโปรโตคอลจะถูกวิเคราะห์ด้วย Coloured Petri Net ซึ่งเป็นเครื่องมือในการสร้างและทดสอบระบบ โดยจำลองผู้โจมตีระบบขึ้น 2 สถานการณ์เพื่อแสดงให้เห็นว่าโปรโตคอลการยืนยันตัวตนที่ถูกพัฒนาขึ้นนั้นมีความปลอดภัย นอกจากนั้นผู้วิจัยได้พัฒนาโปรแกรมต้นแบบของกระบวนการการยืนยันตัวตนขึ้น เพื่อตรวจสอบความถูกต้องในการทำงานของระบบอีกด้วย

71 หน้า