

**A PROTOTYPE TOOL FOR SECURITY AND RISK
ASSESSMENT IN HOSPITAL IT SYSTEM**



SURAPOL RUAYSUNGNOEN

**A THEMATIC PAPER SUBMITTED IN PARTIAL
FULFILLMENT OF THE REQUIREMENTS FOR
THE DEGREE OF MASTER OF ENGINEERING
(COMPUTER ENGINEERING)
FACULTY OF GRADUATE STUDIES
MAHIDOL UNIVERSITY**

Copyright by Mahidol University

COPYRIGHT OF MAHIDOL UNIVERSITY

A PROTOTYPE TOOL FOR SECURITY AND RISK ASSESSMENT IN HOSPITAL IT SYSTEM

SURAPOL RUAYSUNGNOEN 5537199 EGCO/M

M.Eng. (COMPUTER ENGINEERING)

THEMATIC PAPER ADVISORY: SURATOSE TRITILANUNT, Ph.D.,
NOPPADOL WANICHWORANANT, Ph.D., KONGLIT HUNCHANGSITH, Ph.D.

ABSTRACT

The purpose of this study is to propose a security risk analysis process for an IT security system at a hospital. The thesis uses computer security tools to support risk evaluation process. These tools were developed based on the study of standard and best practices of security risk assessment programs used in information system. Moreover, the security assessment was performed using a penetration testing technique that included key processes such as Risk Assessment and Vulnerability Verification along with others factors for supporting this researcher's risk analyzing process and computer security tool development.

The process of risk assessment proposed in this thesis was divided into 4 steps: (1) Planning, (2) Analyzing, (3) Developing, and (4) Utilizing. Results from the experiment showed by inputting the outcome from the vulnerability scan and adjusting the scale of business impact of sample hospitals, the tool was able to assess and rate the security risk which reflected the environment of the hospital's information system. Moreover, this tool was able to simulate some examples of exploitation in order to explore and show system flaws and then generate a report to be used as a reference.

KEY WORDS: SECURITY RISK ASSESSMENT / HOSPITAL SECURITY
ASSESSMENT/ SECURITY ASSESSMENT TOOL

155 pages

ต้นแบบเครื่องมือสำหรับการประเมินความมั่นคงปลอดภัยและความเสี่ยงในระบบสารสนเทศ
โรงพยาบาล (A PROTOTYPE TOOL FOR SECURITY AND RISK ASSESSMENT IN
HOSPITAL IT SYSTEM)

สุรพล รวยสูงเนิน 5537199 EGCO/M

วศ.ม.(วิศวกรรมคอมพิวเตอร์)

คณะกรรมการที่ปรึกษาสารนิพนธ์: สุรทศ ไตรดิลาพันธ์, Ph.D., นกมล วณิชวรนนท์, Ph.D.,
คงฤทธิ หันจางสิทธิ์, Ph.D.

บทคัดย่อ

สารนิพนธ์ฉบับนี้นำเสนอการวิเคราะห์ความเสี่ยงความมั่นคงสารสนเทศสำหรับระบบความมั่นคงปลอดภัยสารสนเทศโรงพยาบาล โดยการทดลองใช้ต้นแบบเครื่องมือช่วยสนับสนุนการประเมินระดับความมั่นคงสารสนเทศที่ถูกพัฒนาขึ้นจากการศึกษาวิเคราะห์แนวปฏิบัติและมาตรฐานที่เกี่ยวข้องกับการ ประเมินความเสี่ยงสารสนเทศ และการทดสอบประเมินความมั่นคงปลอดภัยสารสนเทศโดยการประเมินหาช่องโหว่ โดยเลือกขั้นตอนที่สำคัญและพัฒนาเป็นต้นแบบเครื่องมือเพื่อช่วยสนับสนุนขั้นตอนการประเมินจัดลำดับความสำคัญความเสี่ยง (Risk Assessment) และ การทดสอบยืนยันช่องโหว่ (Vulnerability Verification)

โดยงานวิจัยนี้ได้แบ่งขั้นตอนการดำเนินงานออกเป็น 4 ขั้นตอนคือ (1) การวางแผน (2) การวิเคราะห์ (3) การพัฒนาต้นแบบ และ (4) การทดลองนำไปใช้ จากการทดลองใช้ต้นแบบโดยนำเข้าข้อมูลผลลัพธ์ที่ได้จากการตรวจสอบหาช่องโหว่ (Vulnerability Scan) และปรับเพิ่มระดับผลกระทบทางธุรกิจ (Business Impact) ของโรงพยาบาลที่เป็นกรณีศึกษา พบว่าต้นแบบเครื่องมือสามารถช่วยประเมินจัดลำดับความเสี่ยงที่สะท้อนต่อสภาพแวดล้อมจริงของสารสนเทศโรงพยาบาล และเครื่องมือสามารถจำลองตัวอย่างการทดสอบยืนยัน ค้นหาและแสดงช่องโหว่สารสนเทศและสามารถสร้างรายงานเพื่อใช้เป็นแหล่งข้อมูลอ้างอิงได้