SECONDARY ROLE ASSIGNMENT

GUNTAPONG CHOKEJAREONPATTANAGID

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR
THE DEGREE OF MASTER OF SCIENCE
(COMPUTER SCIENCE)
FACULTY OF GRADUATE STUDIES
MAHIDOL UNIVERSITY
2001

ISBN 974-04-0253-4

4237675 SCCS/M : MAJOR : COMPUTER SCIENCE ; M.Sc. (COMPUTER SCIENCE)
KEY WORDS : ROLE-BASED ACCESS CONTROL, SECONDARY RESPONSIBILITY, IMPLICITLY ROLE ASSIGNMENT, EXPERIENCE (STAFF)-BASED ASSIGNMENT, EVENT (PERMISSION)-BASED ASSIGNMENT, ROLE-BASED ASSIGNMENT, ACTIVATING PROTOCOL, PRECISION-BASED PROTOCOL, AND ECONOMIC-BASED PROTOCOL

GUNTAPONG CHOKEJAREONPATTANAGID: SECONDARY ROLE ASSIGNMENT, THESIS ADVISOR: DAMRAS WONGSAWANG, Ph.D. and SUKANYA PHONGSUPHAP, Ph.D.82 P. ISBN 974-04-0253-4

The most well known access control that is currently and widely implemented in commercial products and accepted as the modern access control standard is role-based access control (RBAC). RBAC uses business roles as a set of least permissions for assigning staff to specific tasks while guaranteeing the maintaining of business constraints. However, sometimes we need some permissions from some roles within a limit of time, but sometimes there are no staff with those roles available at that time. Therefore, we need some staff with a secondary responsibility to take permissions to do that job with precise action and on time. The secondary responsibility is a role assigned to the staff, but secondary role staff cannot activate themselves directly without some certain situation occuring. However, the current role assignment in today's access control software such as operating system or workflow management software is explicitly done. The explicit assignment makes the secondary role unsupportable due to violation of the least privileges assumption. We need to extend the flexibility level for access control that is widely implemented in most software by embedding implicit role assignment features and activating protocol to maintain the least privileges assumption.

This thesis classified the secondary role assignment scheme into three types: Experience (Staff)-Based Assignment, Event (Permission)-Based Assignment, and Role-Based Assignment. The focus is on Role-Based Assignment for defining the two activating protocols that support wide-area enterprises. Precision-based Protocol is used for jobs that focus more on precise action than response time. The Economical-based Protocol is used for jobs that concern the response time or the forwarding jobs to other sites that also cause extremely high cost. The prototype of the proposed model has been simulated and tested with incoming calls of the telephone system.

The results have been analyzed and evaluated. The simulation showed that the prototype performed satisfactorily and can be implemented with the actual system. Finally, future work for further development are also suggested.

4237675 SCCS/M : สาขาวิชา: วิทยาการคอมพิวเตอร์; วท.ม. (วิทยาการคอมพิวเตอร์)

กันตพงศ์ โชคเจริญพัฒนกิจ : การมอบหมายภาระรับผิดชอบรอง (SECONDARY ROLE ASSIGNMENT), คณะกรรมการควบคุมวิทยานิพนธ์: ดร.ดำรัส วงศ์สว่าง และ ดร.สุกัญญา พงศ์สุภาพ . 82 หน้า.

ISBN 974-04-0253-4

**ในปัจจุบันนี้ระบบควบคุมการใช้งานด้วยบทบาทในองค์กรได้ถูกอ้างอิงในผลิตภัณฑ์จนได้รับการยอมรับว่าเป็นมาตรฐานระบบควบคุมการใช้งานสมัยใหม่ ระบบควบคุมการใช้งานชนิดอ้างอิงบทบาทในองค์กรนี้อาศัยเงื่อนไขของบทบาทของบุคคลากรในการดำเนินธุรกิจในการจัดสร้างเป็นสิทธิในการใช้งานของผู้ใช้งานแต่ละคนเพื่อทำงานในแต่ละหน้าที่ โดยยังสามารถรับประกันได้ว่าเงื่อนไขหรือกฎเกณฑ์ในองค์กรยังคงสามารถรักษาไว้ได้ แต่อย่างไรก็ตาม ในบางชั่วขณะเราอาจต้องการการกระทำจากบุคคลในบางบทบาทอย่างเร่งด่วนแต่กลับไม่มีผู้ใช้งานในบทบาทนั้นอยู่ในระบบเลยในเวลานั้น ดังนั้นเราจึงต้องการให้ผู้ใช้งานระบบบางคนที่ได้รับภาระรับผิดชอบรองในการจัดการกับการกระทำนั้นๆ โดยเชื่อมั่นว่าผู้ใช้งานเหล่านั้นจะต้องสามารถกระทำภาระงานได้อย่างถูกต้องและทันการณ์ ซึ่งภาระรับผิดชอบรองนี้เป็นบทบาทที่มอบหมายให้แก่กลุ่มผู้ใช้งานแต่ไม่อนุญาตให้พวกเขาเป็นผู้สามารถกระทำงานบนภาระรับผิดชอบรองได้โดยตรงเว้นแต่มีสถานการณ์บางอย่างเกิดขึ้น แต่ทว่าระบบการมอบหมายบทบาทที่มีในระบบปฏิบัติการหรือซอฟต์แวร์ระบบงานบริหารสิทธิต่างๆในปัจจุบันเป็นการมอบหมายแบบโดยตรงทำให้ระบบภาระรับผิดชอบรองไม่สามารถกระทำได้เนื่องจากกระทบกับข้อสมมติฐานพื้นฐานเกี่ยวกับการให้สิทธิ์ให้น้อยที่สุดที่จะทำงานได้ เราจึงต้องการเพิ่มความยืดหยุ่นในการทำงานของระบบซอฟท์แวร์เหล่านั้นโดยวิธีการเพิ่มคุณสมบัติการมอบหมายภาระรับผิดชอบรองแบบโดยนัยและระบบการอนุมัติสิทธิ์เพื่อที่สมมติฐานพื้นฐานเกี่ยวกับการให้สิทธิ์ให้น้อยที่สุดที่จะทำงานได้ยังคงถูกรักษาไว้ ในวิทยานิพนธ์ฉบับนี้เราจะอธิบายถึงลักษณะการมอบหมายภาระรับผิดชอบรองสามรูปแบบ คือ ระบบอ้างอิงประสบการณ์หรือตัวผู้ใช้ ระบบอ้างอิงเหตุการณ์หรือลักษณะสิทธิ และระบบอ้างอิงบทบาท โดยเราจะเน้นไปที่ระบบอ้างอิงบทบาทเป็นหลักเพื่อที่จะอธิบายระบบการอนุมัติสิทธิที่ยังคงสนับสนุนลักษณะองค์กรแบบข้ามชาติคือ ระบบอนุมัติสิทธิแบบเน้นความถูกต้องของผลลัพธ์ สำหรับงานที่เน้นความถูกต้องมากกว่าเวลาในการตอบสนอง และระบบอนุมัติสิทธิแบบเน้นความประหยัด สำหรับงานที่เน้นเวลาในการตอบสนองมากกว่าความถูกต้อง หรือในกรณีที่การถ่ายโอนงานข้ามพื้นที่มีต้นทุนสูงเกินไป ลักษณะการมอบหมายภาระรับผิดชอบรองได้ถูกทดสอบในสถานการณ์สมมติเกี่ยวกับการรับโทรศัพท์ ซึ่งผลการทดลองได้ถูกวิเคราะห์และสรุปผลว่าลักษณะการมอบหมายภาระรับผิดชอบรองนี้เป็นไปได้ นอกจากนี้ผู้เขียนยังได้แนะนำกระบวนการพัฒนาในอนาคตที่น่าจะเกิดขึ้นไว้ด้วย