BACKWARD AUTHENTICATED MULTI-PARTY KEY AGREEMENT PROTOCOLS

NOPPANUN SUKSOMBOON

ISBN 974-664-956-6

4137847 SCCS/M : MAJOR : COMPUTER SCIENCE ; M.Sc.(COMPUTER SCIENCE)
KEY WORDS : AUTHENTICATION / GROUP KEY AGREEMENT

NOPPANUN SUKSOMBOON : BACKWARD AUTHENTICATED MULTI-PARTY KEY AGREEMENT PROTOCOLS. THESIS ADVISOR: DAMRAS WONGSAWANG, Ph.D, SUKANYA PHONGSUPHAP, Ph.D., 132 p. ISBN 974-664-956-6

Recently, due to the rapid growth of the computer network, many modern application environments involve dynamic peer groups which tend to be relatively small in size and mutate group membership dynamically. Given the openness of today's networks, communication among group members must be secured while maintaining the availability and efficiency of the system. The general secured protocol in context type of dynamic peer groups should be concentrated on secured and efficient group key agreement, secured key authentication, key confirmation and key integrity. All these provide a number of different scenarios of group membership changes that enable addition and exclusion of group members.

This thesis proposed a new protocol, called "Backward authenticated multi-party key agreement protocol" (BA-GDH), to solve security problem for such kind of communication. In order to provide the security services listed above, the BA-GDH protocol performs directly on entities authentication. Each member can verify all previous members in order, and prove that only those members specified can be engaging in the protocol. The first advantage is having ironclad security in a group. Second, it reduces time latency from failure of key generating. The protocol is provably secure against passive adversaries and can be used for practical application. This thesis presented and demonstrated the BA-GDH model in various point of views. The implementation and experimentation under a simulation environment were presented. The discussion and evaluation of the results suggest that further improvement is needed in this area.

4137847 SCCS/M : สาขาวิชา : วิทยาการคอมพิวเตอร์ ; วท.ม.(วิทยาการคอมพิวเตอร์)

นพนันท์ สุขสมบูรณ์ : พิธีการตรวจสอบและรับรองตัวบุคคลที่แท้จริงแบบย้อนกลับของกลุ่มแบบหลายสมาชิกบนข้อตกลงร่วมของกุญแจรหัสลับ (BACKWARD AUTHENTICATED MULTI-PARTY KEY AGREEMENT PROTOCOLS). คณะกรรมการควบคุมวิทยานิพนธ์ : ดำรัส วงศ์สว่าง, Ph.D, สุกัญญา พงษ์สุภาพ, Ph.D, 132 หน้า. ISBN 974-664-956-6

ในปัจจุบันเครือข่ายคอมพิวเตอร์มีการพัฒนาอย่างรวดเร็ว สภาพแวดล้อมของโปรแกรมประยุกต์ใหม่ ๆ มากมาย มีความเกี่ยวข้องกับการทำงานแบบกลุ่มเสมอภาคที่มีการเคลื่อนไหว (กลุ่มที่มีขนาดค่อนข้างเล็ก และมีการเคลื่อนไหวของสมาชิกในการเข้าและออกจากกลุ่ม เกิดขึ้นตลอดเวลา) แต่เนื่องจากระบบเครือข่ายในปัจจุบันเป็นระบบเปิด ดังนั้นการติดต่อสื่อสารระหว่างสมาชิกภายในกลุ่มควรจะมีระบบการรักษาความปลอดภัย และยังคงไว้ซึ่งประสิทธิภาพโดยรวมของระบบ พิธีการรักษาความปลอดภัยทั่ว ๆ ไปที่เกี่ยวข้องกับกลุ่มเสมอภาคที่มีการเคลื่อนไหว ควรจะต้องคำนึงถึงความปลอดภัย และความมีประสิทธิภาพในการจัดการข้อตกลงร่วมของกุญแจรหัสลับ, การตรวจสอบและรับรองตัวบุคคลที่รัดกุม, การมีรหัสลับที่ใช้ยืนยันรหัสที่ถูกต้องและการมีความเป็นอันหนึ่งอันเดียวของรหัสลับ พร้อมกันนั้นมันควรจัดเตรียมเพื่อรับมือกับการเปลี่ยนแปลงของสมาชิก ที่สามารถเข้าและออกจากกลุ่มได้ตามต้องการ

วิทยานิพนธ์ฉบับนี้ได้เสนอพิธีการใหม่เรียกว่า "พิธีการตรวจสอบและรับรองตัวบุคคลที่แท้จริงแบบย้อนกลับของกลุ่มแบบหลายสมาชิกบนข้อตกลงร่วมของกุญแจรหัสลับ" (BA-GDH) เพื่อแก้ปัญหาที่อาจเกิดขึ้นในการติดต่อสื่อสาร นอกเหนือไปจากระบบรักษาความปลอดภัยที่กล่าวมาข้างบนแล้ว พิธีการ BA-GDH ยังกระทำการการตรวจสอบและรับรองตัวบุคคลแบบตรงไปตรงมา กล่าวคือ แต่ละสมาชิกสามารถตรวจสอบและยืนยันการเป็นสมาชิกที่แท้จริงของสมาชิกคนก่อน ๆ ตามลำดับ ทั้งนี้เป็นการพิสูจน์ว่าสมาชิกที่ถูกต้องในกลุ่มเท่านั้นจึงจะเข้าทำงานในพิธีการได้ ประโยชน์ที่ได้รับอย่างแรกคือระบบรักษาความปลอดภัยในกลุ่มมีความแข็งแรงขึ้น อีกทั้งยังลดเวลาในการสร้างรหัสลับในกรณีที่มีการแทรกแซง พิธีการนี้สามารถพิสูจน์ถึงการป้องกันการแทรกแซงจากผู้ไม่ประสงค์ดี และมีแนวทางที่นำไปใช้งานได้จริง วิทยานิพนธ์ฉบับนี้ได้นำเสนอและสาธิตการทำงานของตัวแบบในหลาย ๆ มุมมอง มีการการทดลองภายใต้การจำลองสถานการณ์ พิจารณาและประเมินค่าผลลัพธ์ที่ได้ รวมถึงแนะนำข้อเสนอแนะเพื่อนำไปปรับปรุงต่อไป