CREATION AND ANALYSIS OF THE MESSAGE AUTHENTICATION CODE BY USING KEY CHAINING

PRASERT CHAROENRUNGREUNGDEE

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR
THE DEGREE OF MASTER OF SCIENCE
(COMPUTER SCIENCE)
FACULTY OF GRADUATE STUDIES
MAHIDOL UNIVERSITY
2000

ISBN 974-663-743-6

4037524 SCCS/M : MAJOR : COMPUTER SCIENCE ; M.Sc. (COMPUTER SCIENCE)
KEY WORDS : MESSAGE AUTHENTICATION CODE/ KEY CHAINING
PRASERT CHAROENRUNGREUNGDEE : CREATION AND ANALYSIS OF THE MESSAGE AUTHENTICATION CODE BY USING KEY CHAINING. THESIS ADVISOR : DAMRAS WONGSAWANG Ph.D., SUKANYA PHONGSUPHAP Ph.D., 98 P.
ISBN 974-663-743-6

The main purpose of message authentication code (MAC) is to maintain the integrity of messages normally sent via the communication channel. It is applied to protect the unauthorized alteration of messages and prove genuineness. There are a number of methods to generate MAC currently in use. One of the most well-known and widely used method is cipher block chaining MAC (CBC-MAC). However, it is found that CBC-MAC cannot handle variable-length input messages. This weak point leads to the vulnerability of CBC-MAC in that a message may be forged.

This research proposes an improved model, called Key Chaining MAC (KC-MAC), to solve the problem found in CBC-MAC. KC-MAC removes the weak exclusive-or of CBC-MAC so that an adversary is not allowed to choose any block to forge a message. To strengthen KC-MAC, key chaining is also added. The key chaining feature causes a secret key of the next block message to be changed dynamically, so it is harder to break KC-MAC generation.

The prototype of the proposed model has been developed, implemented, tested and analyzed with the employment of Data Encryption Standard (DES). The MAC generation results show that KC-MAC can solve the problem found in CBC-MAC. The generating performance is almost the same for both methods. However, KC-MAC has more reliability and strength than CBC-MAC. The detail of KC-MAC has been presented and implemented. Its results have been discussed. Finally, improvements of the model have been suggested.

4037524 SCCS/M : สาขาวิชา : วิทยาการคอมพิวเตอร์ ; วท.ม. (วิทยาการคอมพิวเตอร์)

ประเสริฐ เจริญรุ่งเรืองดี : การสร้างและวิเคราะห์รหัสเพื่อป้องกันการปลอมแปลงข้อความโดยการใช้การโยงกุญแจรหัสลับ (CREATION AND ANALYSIS OF THE MESSAGE AUTHENTICATION CODE BY USING KEY CHAINING) คณะกรรมการควบคุมวิทยานิพนธ์: ดำรัส วงศ์สว่าง, Ph.D., สุกัญญา พงษ์สุภาพ, Ph.D., 98 หน้า. ISBN 974-663-743-6

เป้าหมายที่สำคัญของการนำรหัสป้องกันการปลอมแปลง (message authentication code หรือ MAC) มาใช้คือ เพื่อรักษาให้ข้อมูลมีความถูกต้องสมบูรณ์ในขณะที่เดินทางผ่านช่องสื่อสาร วิธีนี้ได้ถูกนำไปประยุกต์ใช้เพื่อป้องกันการแก้ไขข้อมูลจากผู้ที่ไม่มีสิทธิ์ และยังใช้พิสูจน์ว่าข้อมูลใดที่เป็นของจริง ในปัจจุบันมีการนำเสนอวิธีการสร้างรหัสนี้หลายวิธี วิธีหนึ่งที่คนส่วนมากรู้จักและนิยมใช้คือ Cipher Block Chaining (CBC-MAC) ต่อมาได้มีนักวิจัยศึกษาและพบว่า CBC-MAC ไม่สามารถให้ความปลอดภัยเมื่อความยาวของข้อมูลมีขนาดที่ไม่คงที่ จากจุดอ่อนนี้จึงนำไปสู่ข้อด้อยของ CBC-MAC ที่จะถูกปลอมแปลงข้อมูล

งานวิจัยฉบับนี้ จึงได้เสนอวิธีที่สามารถแก้ปัญหาของ CBC-MAC ได้ซึ่งเรียกว่า Key Chaining MAC (KC-MAC) วิธีนี้สามารถแก้ปัญหาของ CBC-MAC ได้โดยการยกเลิกการทำ exclusive-or ซึ่งเป็นจุดอ่อนของ CBC-MAC ส่งผลให้ผู้บุกรุกไม่สามารถเลือกข้อมูลที่จะมาทำการปลอมแปลงได้ และเพิ่มจุดแข็งคือ การนำผลลัพธ์ที่ได้จากการเข้ารหัสของกลุ่มข้อมูลไปโยงหรือป้อนกลับ (feedback) เพื่อเป็นกุญแจรหัสลับสำหรับเข้ารหัสข้อมูลส่วนต่อๆไป โดยที่ผู้บุกรุกไม่รู้ค่าที่ถูกป้อนกลับ วิธีนี้เรียกว่า การโยงกุญแจรหัสลับ (key chaining)

KC-MAC ใช้ Data Encryption Standard (DES) เป็นต้นแบบในการพัฒนา ทดสอบและวิเคราะห์ ซึ่งผลของการทดลองแสดงให้เห็นว่า KC-MAC สามารถแก้ปัญหาของ CBC-MAC ได้ ถึงแม้ว่าประสิทธิภาพของทั้งสองวิธีจะใกล้เคียงกันแต่ KC-MAC เป็นวิธีที่มีความน่าเชื่อถือมากกว่า CBC-MAC งานวิจัยนี้ได้เสนอรายละเอียดของ KC-MAC การทำให้เกิดผลและการอภิปรายผลลัพธ์ที่ได้ นอกจากนี้ยังได้แนะนำถึงการปรับปรุง KC-MAC ให้ดีขึ้น