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.