Tribhuvan University

Institute of Science and Technology

Performance Analysis of Cipher Block Chaining Message Authentication Code (CBC MAC) and its Variants

Dissertation

Submitted to:

Central Department of Computer Science and Information Technology

Tribhuvan University, Kirtipur, Nepal

In partial fulfillment of the requirements

For the Master's Degree in Computer Science &Information Technology

By

Chhetra Bahadur Chhetri

Feb 25, 2014

Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science and Information Technology

Supervisor's Recommendation

We hereby recommend that this dissertation prepared under my supervision by **Chhetra Bahadur chhetri** entitled **"Performance Analysis of Cipher Block Chaining Message Authentication Code (CBC MAC) and its Variants"** in partial fulfillment of the requirements for the Master's Degree in Computer Science &Information Technology be processed for the evaluation.

…….

Asst.Prof.Nawaraj Paudel

Head of Department (HOD)

Central Department of Computer Science and Information Technology

Kritipur, Kathmandu, Nepal

(Supervisor)

Date: ……

Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science and Information Technology

Declaration

"I, Chhetra Bahadur Chhetri, declare that the Master by Research thesis entitled Performance Analysis of Cipher Block Chaining Message Authentication Code (CBC MAC) and its Variants contain no sources other than listed, this thesis is my own work."

…….

Chhetra Bahadur Chhetri

Feb 25, 2014

Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science and Information Technology

LETTER OF APPROVAL

We certify that we have read this dissertation and in our opinion it is satisfactory in the scope and quality as a dissertation in partial fulfillment of the requirements for the Master's Degree in Computer Science &Information Technology.

Evaluation Committee

…….

Asst.Prof.Nawaraj Paudel

Central Department of Computer Science and Information Technology

Kritipur, Kathmandu, Nepal

(HOD)

…….. ……

(External Examiner) (Internal Examiner)

Date : ……

Acknowledgments

It's a pleasure for me to thank my principal supervisor, **Asst.Prof.Mr.Nawaraj Paudel**, Head of Computer Science & IT Department, TU (Kathmandu, Nepal) for his constant encouragement, support and advice.

I greatly acknowledge respected teachers **Prof. Dr. Shashidhar Ram Joshi, Prof. Dr. Subarna Shakya, Mr.Dheeraj Kedar Pandey, Mr. Jagdish Bhatta , Mr. Arjun Singh Saud, Mr. Bishnu Gautum, Mr.Bikash Balami, Mrs. Lalaita Stapit** of CDCSIT, TU, for providing valuable suggestion and huge knowledge and inspirations. I would like to thank my friends and family for their encouragement and support. I would like to give my special thanks to my friends **Mr. Prakash Datt Bhatt** and **Mr. Ram Krishna Dahal** for providing wonderful environment and resources to complete this work.

Abstract

The cryptographic algorithms employed in internet security must be able to handle packets which may vary in size over a large range. Most of the cryptographic algorithms process messages by partitioning them into large blocks. Due to this fact the messages have to be prepared by padding the required amount of zero bits to get an integer number of blocks. This process contributes a considerable overhead when the short messages are more dominant in the message stream. Here in this thesis, analyses is focused on the performance of different message authentication code generator algorithm based on cipher block. These all variants of cipher based must have to share symmetric key before creating message authentication code. All variants of CBC MAC are implemented in JAVA. The result of empirical performance shows that two variants namely TMAC perform better for AES Encryption algorithm in larger size otherwise EMAC show the better result with the Triple DES symmetric algorithm. The result shows that, when consider only on the performance aspect. Cycle/byte is calculated for comparing different variants of CBC MAC. Cycle/byte is decreased when input size of message is increased. Advanced Encryption Standard (AES) algorithm shows good performance than TDES and it has better security features than DES. CBC-MAC is likely to be standardized as an AES mode of operation.

TABLE OF CONTENTS

List of Figures

LIST OF TABLES

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
API	Application Programming Interface
CBC MAC	Cipher block chaining Message Authentication Code
DES	Data Encryption Standard
EMAC	Encrypted Message Authentication Code
JVM	Java Virtual Machine
IDE	Integrated Development Environment
MAC	Message Authentication Code
OMAC	One- key Message Authentication Code
PKI	Public Key Infrastructure
PMAC	Parallelizable Message Authentication Code
SHA	Secure Hash Function
TDES	Triple Data Encryption Standard
TMAC	Two –key Message Authentication Code