Study of Avoiding Length Extension attack on MD Based Secret Prefix Message Authentication Code

B.H.A.J. Premadasa
(Reg. No.: MS20903060)
M.Sc. in IT
Specialized in Cyber Security

Supervisor : Dr. Lakmal Rubasinghe

October 2021

Department of Computer Science
Faculty of Graduate Studies and Research
Sri Lanka Institute of Information Technology

Abstract

The integrity of the message can be violated intentionally or unintentionally caused by means of natural phenomena or interceptions of malicious actors. Changes in message integrity caused by natural reasons can be corrected using various error correction mechanisms. Message Authentication Code is being widely used in order to check the integrity of a message. Using Message Authentication Code, the receiver can check whether the message is modified or changed during the transmission process. Message Authentication Code comes handy when detecting integrity violations by malicious actors. The integrity check is done by calculating special values which can be only obtained by using the original message. The calculated hash value by the sender is appended at the end of the message and transmitted to the receiver. The receiver gets the message and calculates the hash value using the same techniques used by the sender. By comparing accumulated hash value with the hash value sent by the sender, any integrity violation can be identified. But the hashing algorithms based on Merkle–Damgård construction are vulnerable to length extension attacks. To address this vulnerability, Secure Hash Algorithms are introduced. The purpose of this study is to develop a novel algorithm to avoid length extension attacks on MD based message authentication algorithm.

Keywords – Authentication, Merkle–Damgård construction, Message Authentication, Length Extension.

Contents