INFORMATICS INSTITUTE OF TECHNOLOGY

INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER

Evaluation of brute-force techniques to improve the defence against brute-force induced attacks

A dissertation by

D.D.M.S.M.B.Dissanayake

Supervised by

Mr. Sithira Hewaarachchi

Submitted in partial fulfilment of the requirements for the Master of Science in Cyber Security and Forensics degree at the University of Westminster

September 2022

Abstract

If someone wants to securely store data indefinitely, it is nothing more than encrypting it with a key. However, this has its own limitations where an attacker could try many keys until he/she breaks the encryption directly by guessing the right key. Year by year, the processing power increases from mobile processors to quantum computers. And the brute-force attack on encrypted data is also consuming very less time in the current state; compared with the techniques, technologies and resources used in earlier years. And in the future, in the worst case, there will be a time, where the HTTPS traffic might be brute-forced in a considerable time. The real threat of this is, the brute-force attacks are completely relying on the processing power rather than the attacker's skills. Alternative strategies must be taken into consideration in order to prevent or at least minimise being exposed to brute-force assaults as processing power grows dramatically over time, along with cloud and distributed computing. The goal of this research is to develop a brute-force prevention technique regardless of encryption standard that will at the very least guarantee that the encrypted content cannot be decrypted throughout the typical human lifetime, regardless of how powerful the CPU or GPU is.

Keywords: Brute-force, Encryption, Quantum Resistant, Cryptography