Analytical and Experimental Analysis of Hash Algorithms in Authentication Practices

NGUYEN Thi Ha Trang
BUI Tuan Thanh
NGUYEN Minh Huong

Abstract

Password-based authentication is still widely used, although weak and reused passwords remain a common source of security risks. For this reason, evaluating the hash functions and password hashing methods used in authentication systems is important for understanding their practical security. This work studies how different hashing approaches behave in realistic password-protection scenarios and how their observed behavior compares with theoretical expectations.

The main contribution of this work is an experimental evaluation of hash functions used in practice. The study compares experimental observations with theoretical models in order to assess how well these models reflect the behavior of hashing methods under password-guessing attacks. Instead of treating security only as a theoretical property, the work focuses on the gap between analytical assumptions and practical performance.

The objective is to provide a clearer view of the security and computational trade-offs of different hashing approaches in password-based authentication. The results support a more practical understanding of how hash functions and password hashing schemes should be evaluated and selected for real authentication systems.