International Journal of Interdisciplinary Telecommunications and Networking
Volume 12 • Issue 4 • October-December 2020

Performance and Security Tradeoffs in Cryptographic Hash Functions

Sultan Almuhammadi, King Fahd University of Petroleum and Minerals, Saudi Arabia
Omar Mohammed Bawazeer, King Fahd University of Petroleum and Minerals, Saudi Arabia

ABSTRACT

A cryptographic hash function is an important component used in many applications, such as blockchain, authentication, data integrity, and digital signature. With the rapid increase in usage of mobile devices, more attention goes towards the tradeoffs between performance and security of cryptographic hash functions on mobile devices due to their limited computational power. The researchers in this paper study the most common cryptographic hash functions and highlights the tradeoffs between their performance and security. The hash functions considered in this study are MD4, MD5, Whirlpool, and the hash functions in the SHA family. The security of these hash functions is compared based on recent attacks in terms of collision resistance, preimage attacks, and sensitivity analysis. While the performance is tested on different input block sizes, useful observations and recommendations are made based on the results of this study.

KEYWORDS

Authentication, Collision Resistance, Integrity, Secure Hash Function, Sensitivity Test

1. INTRODUCTION

The importance of cryptography and information security has grown rapidly to meet security goals in the digital world. As networking and communication fields grow, computer specialists have developed many tools to satisfy the needs of security for individuals and organizations. With today's usage of mobile devices, wireless network become essential. However, the limited resources in mobile devices and wireless network creates the need to study the tradeoffs between performance and security in these technologies.

Improvements of security and cryptographic tool include symmetric/asymmetric-key encipherments, cryptographic hash functions and many other tools for different applications (Sobti & Geetha, 2012; Forouzan, 2008; Stallings, 2006). On the other hand, the development of information security coincided with the improvement of attacking techniques that try to get access to confidential information, harm the system, etc. (Forouzan, 2008).

Besides network security, secure hashing functions have many applications. The security of data should be maintained both when it's static or dynamic (Kishore & Kapoor, 2016). For static security, on the computing devices, the stored data must be legitimately encrypted and controlled (Kishore &

DOI: 10.4018/IJITN.2020100103

Kapoor, 2016). For dynamic security, suitable network security actions must be set up to ensure the information through its transmission (Kishore & Kapoor, 2016).

Cryptographic hash functions are used in many services and mechanisms such as Data Integrity, Authentication, Non-repudiation, Digital Signature, Blockchain, and so on. A system needs to guarantee at least one of these relying on the security prerequisites for a specific system. The cryptographic hash functions techniques are used to accomplish some of these security services. Cryptographic hash functions are designed in two ways: one way is to make it from scratch (like MD5, MD6, SHA-x) and the other way is based on Block cipher (like Whirlpool) (Forouzan, 2008). Unfortunately, there are several ways to attack the hashed information by using some attacking techniques such as preimage attack, second preimage attack, and collision attack (Forouzan, 2008; Stallings, 2006).

This paper presents a detailed study on the current hash functions, including their strengths and weakness points. In addition, two experiments are conducted to test the performance of the hash functions and their sensitivity to the input change. Based on the results of this study, suggestions and useful recommendations are provided for mobile devices and wireless networks.

2. CRYPTOGRAPHY AND NETWORK SECURITY

Cryptography performs a significant part in securing the confidential information in different applications such as medical databases, e-commerce, email, e-banking, etc. It also plays a major role in network security applications, including: confidentiality, integrity, and availability (Forouzan, 2008).

Confidentiality: ensures the privacy of data in such a way that no one can read the message unless authorized.

Integrity: means that any change or modification must be done by the authorized entities.

Availability: means that the information must be available for the authorized entities.

2.1. Cryptographic Hash Functions

A cryptographic hash functions is one-way function that takes an input of a variable-length and produces a message digest (or hash-value) which has a fixed output-size. Thus, $H(M) = h$ (Forouzan, 2008; Stallings, 2006).

A cryptographic hash function, H shown in Figure 1, has the following properties: (Sobti & Geetha, 2012)

1) The input data or message M has a variable length.
2) The output (message digest) of H has a fixed output-size $|h|$
3) It is computationally infeasible to find x for a given H and $H(x)$.
4) It is computationally infeasible to find x and y such that $H(x) = H(y)$.

To produce the message digest, all cryptographic hash functions now are using iteration. So, the long message input of an arbitrary size is divided into k fixed size segments that will be compressed by a compression function which accepts an n-bits input to produce m-bits output, where $n \geq m$ typically, and iterated k times to create the output (Forouzan, 2008). Depending on the designing of compression function, the cryptographic hash functions are classified into two types. The first one is made from scratch, which originally designed for the hash functions like the Message Digest (MD) family (MD2, MD4, MD5, and MD6) and the Secure Hash Algorithms (SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512). The second type is the hash functions that based on block ciphers such as Whirlpool (Forouzan, 2008; Stallings, 2006). Table I summarizes the details of the most common hash functions.

There is a tradeoff between the security of the hash function and its performance. Many cryptographic hash functions nowadays have different strength, and they are typically categorized