Project Hash Attack - Report

Sitharthan G Ramalingam
Reviewed by : Zackery Whitscell

Introduction

Many security system's core building blocks include cryptographic hash algorithms. They are employed to produce digital signatures, check the accuracy of data, and safely store passwords. A strong hash function should be protected against preimage and collision attacks.

Here, When an attacker discovers two distinct messages with the same hash value, it is known as a collision attack. An attacker launches a preimage attack when they discover a message that hashes to a specific value, Where n is the number of bits in the digest, the theoretical difficulty of implementing a collision attack on a hash function is around 1.1774*2^(n/2) and the Preimage attacks on hash functions have a theoretical complexity of about 2n.

In this experiment , We tested a number of collision and preimage attacks on the SHA-1 hash algorithm using various bit sizes in this research. Data was obtained on how many tries each attack required to succeed.

Methodology

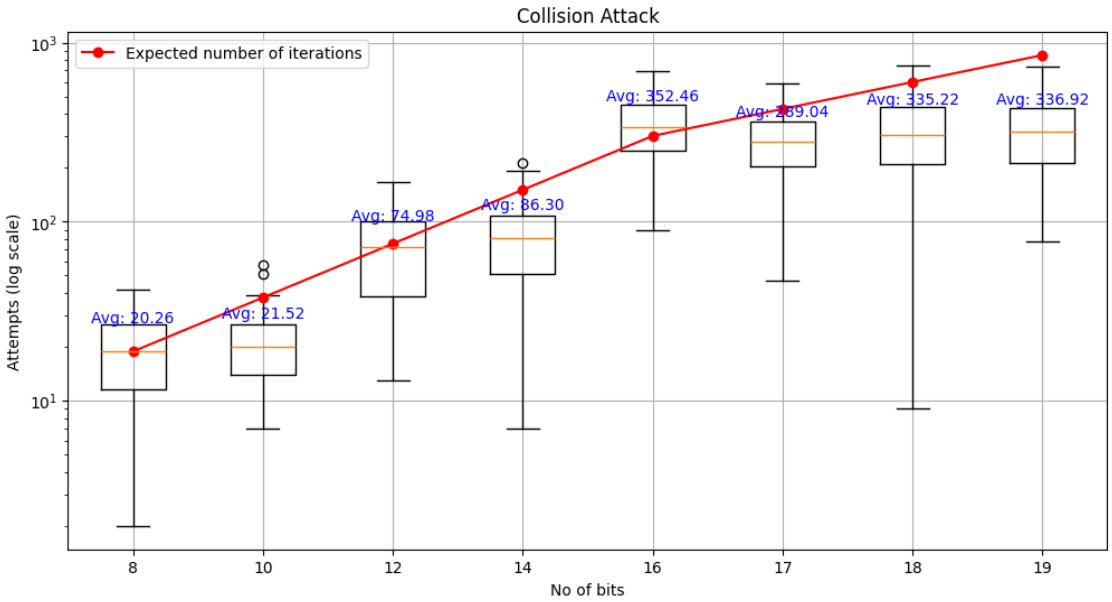
We developed a wrapper for a particular SHA-1 implementation using the Python hashlib module. This wrapper receives as inputs the string to hash and the requisite amount of bits (n). The result was a SHA-1 hash of the supplied string that had been truncated to the specified number of bits.

We carried out a number of collision and preimage attacks using this wrapper using various bit sizes. Between 8 and 32-bit sizes, we evaluated at least 8 distinct bit sizes. We chose the following bit sizes: 8,10,12,14,16,17,18,19.

For each bit size, we collected 50 samples for successful collision, Where we searched for a collision or preimage for each trial for a random string. We recorded the number of attempts each attack required to succeed and plotted them in a Box plot graph to compare the results with the theoretically expected results.

Below are the graphs we generated through our experiment data,

Graphs 1 :

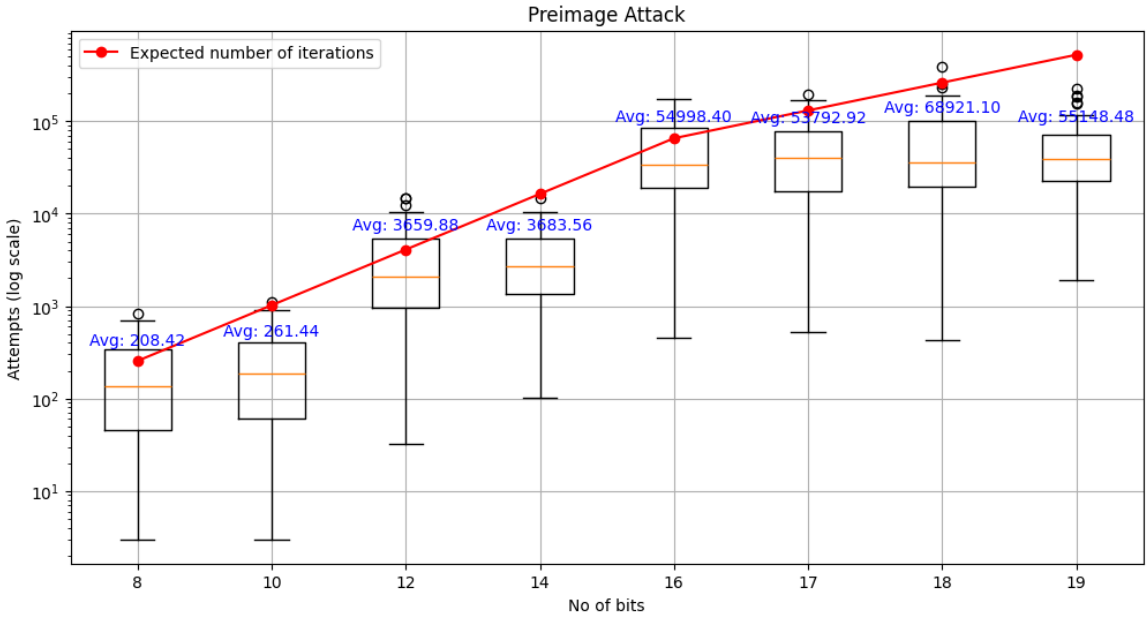


Description: Graph 1 illustrates the number of attempts needed to identify two distinct inputs that result in the same hash output with different bit sizes. The y-axis of the graph, which is presented on a logarithmic scale, displays the successful collision attacks in powers of 10 and the x-axis of the graph presents a number of different bit sizes used for the attack.

Analysis:

Our results show that the difficulty of performing a collision attack on SHA-1 increases with the bit size of the digest. The graph also states that the collisions are possible in SHA-1. Here, we can also see that for an 8-bit hash digest, the average number of attempts needed for a collision is 20. This is consistent with the theoretical difficulty of this attack, which is 1.1774 * 2^n/2, where n is no of bits in the hash digest. We can also see that, This remains the same for all bit sizes used for this experiment.

Graph 2:



Description: Graph 2 illustrates the number of attempts needed to identify the identical hash of a target where the hash has different bit sizes. The y-axis of the graph, which is presented on a logarithmic scale, displays the successful collision attacks in powers of 10 and the x-axis of the graph presents a number of different bit sizes used for the attack.

Analysis:

Our results show that the difficulty of performing a preimage attack on SHA-1 increases exponentially with the bit size of the digest. The graph also states that the preimage attack is possible in SHA-1. Here, we can also see that for an 8-bit hash digest, the average attempt needed for a collision is 208 This is consistent with the theoretical difficulty of these attacks, which is 2^n, where n is no of bits in the hash digest. We can also see that, This remains the same for all bit sizes used for this experiment.

Conclusion:

We have conducted a series of collision and preimage attacks on the SHA-1 hash function at different bit sizes. Our results show that the difficulty of performing these attacks increases with the bit size of the digest. Also, We can see that the difficulty of a preimage attack is comparatively higher than a collision attack. Given the vulnerabilities demonstrated in these attacks, SHA-1 is generally considered deprecated and unsuitable for cryptographic security purposes.