Name: Isai Mercado Oliveros

Net id: misaie

Date: September 17, 2015

Collision Attack and Preimage Attack

Hash functions are function used in computer security to sign up information, such as digital works, or passwords. They are one-way functions which means that they take an input and produce an output that cannot be taken to produce the initial input. On the contrary, Ciphers can encrypt an input then produce an output which can then be taken to produce the initial input again. However, they cannot sign information perfectly due to the fact that several inputs may produce the same output therefore a signature maybe reproduced by a fake input. Two of those weakness are called collision attack, and preimage attack. This two weaknesses were tested, and the result are presented after we define collision attack and preimage attack.

Collision resistance measures how difficult it is to pick two inputs that produce the same output.

A Collision Attack happens when the attacker finds two inputs that hash to the same output. The attacker does not care about the hash value. However, he only cares that the two inputs hash to the same value. An example on how this attack may be used is to modify a contract. Lets say that someone commits to pay 50,000 dollars for a car, and then the document is sign with a hash function. However, the buyer finds that the same contract with the amount of 5 dollars hashes to the original value, so he pays 5 dollars and uses the 5 dollars contract as a signature.

In addition, a collision attack may be used to produce a preimage attack. A preimage attack is when the attacker intercepts the hash value of someone else signature, and they tries to find some other input that produces that same hash value. If successful, the attacker will now have a token that will produce the same signature. For instance, lets say that a computer user is in a public network and he enters his username and password for his banking account; however, the hash value of his banking authentification is intercepted by an attacker, who knows the banking hash function. The attacker would try to find a combination of generated username, and a generated password that produces the same hash value as the computer user banking signature. The attacker would then enter the generated username and password to sign up in the online account which will work because they were hashed to the same value.

The main difference between a collision attack and a preimage attack is that in the collision attack we do not care about the hash value produced by two inputs. However, we care about the fact that two inputs hash to the same value. This was exemplified by the two contracts with the same hash signature. On the other hand, in a preimage attack we do not care about the inputs, but we care about the hash value that they both produce. This attack was exemplified by the public network attacker who only cares for a way to reproduced the intercepted hash value.

Experiment

This experiment is divided in two sections. The first section tries 10,000,000 times to find a collision hash on 10 randomly created words. The second section tries 10,000,000 to find a word that hashes to 1 of 10 randomly created hash values.

The code is very similar; however, the wanted element differs. In the collision attack test we care about the hash value of the word that collides with the initial word's hash value, and in the preimage attack test, we care about the word whose hash value collided to the initial word's has value.

The probability of finding a collision is very small (0.000006%). In average, there were only 4-6 collisions on 100,000,000 tries using hash values of 24 bits. In addition, for a BYU lab computer, find a collision on a 24 bits hash value took 7.5 Seconds. This time increases exponentially which is what gives hash functions its strength. For instance, according to <http://www.unixwiz.net/techtips/iguide-crypto-hashes.html> “512 bits of hash holds 1.34 x 10154 possible values, which is far, far more than the number of hydrogen atoms in the universe”. If 24 bits had a probability of 0.000006%, I imagine that finding a hash collision in a hash value of 512 bits is almost impossible.

Results

Collision Tests Logger Output

There was a collision on test 1 out of 10 tests

after 6291272 collision tries

User Password: 0xCFD151CD2D7DC89741B1

Random Word: 0xD6CC6F3F313A8B053A7C

Collision Hash: 0x6059FF

Time: 9.037256796E9 nano seconds

There was a collision on test 2 out of 10 tests

after 6332160 collision tries

User Password: 0xB11E095307812F1A2978

Random Word: 0x54F36B9F8A5A7D4B73F1

Collision Hash: 0x623F6E

Time: 8.893656968E9 nano seconds

There was a collision on test 9 out of 10 tests

after 4686937 collision tries

User Password: 0x1A12A4DB1D30C0F62A21

Random Word: 0xA0BED69DC438689859D4

Collision Hash: 0xA1AF0C

Time: 6.520160199E9 nano seconds

There was a collision on test 9 out of 10 tests

after 5674979 collision tries

User Password: 0x1A12A4DB1D30C0F62A21

Random Word: 0xEC90BCB71B78A01A67E4

Collision Hash: 0xA1AF0C

Time: 1.374395272E9 nano seconds

There was a collision on test 10 out of 10 tests

after 2231586 collision tries

User Password: 0x2E0C681F40F8B336D15D

Random Word: 0xF0A2A33B2C923452EA07

Collision Hash: 0x65242D

Time: 3.103303187E9 nano seconds

There was a collision on test 10 out of 10 tests

after 9303397 collision tries

User Password: 0x2E0C681F40F8B336D15D

Random Word: 0xBA01E9AE5D1AAACB93AC

Collision Hash: 0x65242D

Time: 9.879696848E9 nano seconds

Collision tests finished after 140.061782603 seconds

What is the probability of having two words with the same hash value when that a value has 24 bits after 10,000,000 random Words?

Probability: 0.00000600%

What is the avarage time to find a collision per word?

Average time: 7.2647462528 Seconds

Preimage Tests Logger Output

There was a collision on test 1 out of 10 tests

after 1274189 collision tries

Unknown Password Hash: 0x6C19BF

PreImage Password: 0x15DE2BDAAF3CA329D5ED

Time: 1.804262407E9 nano seconds

There was a collision on test 1 out of 10 tests

after 4048533 collision tries

Unknown Password Hash: 0x6C19BF

PreImage Password: 0x24D5A9CF69D93FF60903

Time: 3.910066071E9 nano seconds

There was a collision on test 1 out of 10 tests

after 9928745 collision tries

Unknown Password Hash: 0x6C19BF

PreImage Password: 0xBE2ABB18E7229BFB4165

Time: 8.409269124E9 nano seconds

There was a collision on test 6 out of 10 tests

after 295183 collision tries

Unknown Password Hash: 0x0561A6

PreImage Password: 0x37C0C4A54045A44A84E4

Time: 4.14036886E8 nano seconds

There was a collision on test 6 out of 10 tests

after 3220136 collision tries

Unknown Password Hash: 0x0561A6

PreImage Password: 0x2B9A87A2764CA6C47563

Time: 4.109557138E9 nano seconds

There was a collision on test 6 out of 10 tests

after 4529101 collision tries

Unknown Password Hash: 0x0561A6

PreImage Password: 0x40A52C25AA9785EBAB30

Time: 1.835144355E9 nano seconds

There was a collision on test 10 out of 10 tests

after 4696243 collision tries

Unknown Password Hash: 0xD0EAC2

PreImage Password: 0xD14CF3D503D962652C51

Time: 6.596883922E9 nano seconds

PreImage tests finished after 140.251745293 seconds

What is the probability of finding a preImage password on an intercepted hash of 24 bits after 10,000,000 random Words?

Probability: 0.00000700%