Danny North

CS 465

9/18/15

Fred Clint

Lab 2 Report

Part 1 - Collision:

In order to test for collision, I use an arbitrary string and keep using that string in order to find out the total time complexity as the time difference goes up from the previous test. As I increment my original string, I add hashes to a list that don't match the original string's hash, only after checking against the original hash. Once I find a match, I end the program and count the array length. I test one nibble at a time (4 bits).

Bits	Time (Seconds)	Original String	Collision String	Array Length	Collision Hash
4	0.000006	'1324981'	'1324989'	7	0xd
8	0.00030	'1324981'	'1325030'	48	0xce
12	0.00074	'1324981'	'1325113'	131	0x321
16	0.00441	'1324981'	'1325508'	526	0x8162
20	0.02351	'1324981'	'1326640'	1658	0xed2e4
24	0.62056	'1324981'	'1334545'	9563	0xe76c9e
28	1.26774	'1324981'	'1339358'	14376	0xd95f164
32	71.0260	'1324981'	'1434617'	109635	0xddfabfde
36	374.771	'1324981'	'1570157'	245175	0x78a62155d

As you can see, the time complexity for the worst case is 2 ^ (n/2). It would be improbable to try and continue with larger bit values unless I wanted to wait for minutes, hours, days, etc....

Part 2 - Pre-Image Attack:

To test this, I again keep the same string value and try to find a different value that hashes to that same value. Keeping the same string value helps me determine the worst case time complexity as the number of bits rises.

Bits	Time (Seconds)	Original String	Collision String	Collision Hash
4	0.000148	'cs465IsDaBest'	'31'	0x6
8	0.000159	'cs465IsDaBest'	'31'	0x63
12	0.007099	'cs465IsDaBest'	'2399'	0x63c
16	0.198120	'cs465IsDaBest'	'98850'	0x63c8
20	0.631540	'cs465IsDaBest'	'312332'	0x63c8b
24	9.968218	'cs465IsDaBest'	'4722252'	0x63c8bd
28	258.69490	'cs465IsDaBest'	'124844617'	0x63c8bde

The pre-image complexity is actually worse than the Collision time complexity. This is 2^(n) time complexity, which means I was only able to go up to 28 bits before it became infeasible to continue trying to find the complete hash value.

Conclusion:

Although it is possible to brute force an attack on these types of hashes to try and find out a message or use collision to a hacker's favor, the time complexity is such that a full 128-bit SHA-1 hash would not be feasible (at least for me!!!!) and take a lot of resources and cost a lot of money.