ITIS 6200/8200 Principles of Information Security and Privacy

Weichao Wang

Fall Semester of 2017

Homework 3

Hand out: September 15th, 2017

Due time: September 22nd, 2017 before 11:00 am

1. Alice’s computer stores the files in the following way: for every file F, the computer will calculate the hash value of the file hash(F) and store it after the file. Every time when Alice login, the machine will automatically hash all the files and compare the results to the stored hash values. In this way, if by accident the hard drive is mis-functioning and flips a few bits in a file, Alice can immediately detect it since the hash value will be different. Now an attacker hacks into Alice’s machine and he tries to change several files. The attacker also knows the hash function that the computer uses. Please describe what the attacker needs to do so that the next time Alice login, the machine will not detect the changes. Also, please discuss how we should improve the mechanism to detect such changes.
2. Please draw a binary Merkle’s hash tree with 9 leaf nodes. The leaf nodes are labeled as Leaf1 to Leaf9, which correspond to the hash values of the files F1 to F9, respectively. Now please answer:
   1. For each node in the tree, please label clearly how the hash value is calculated based on its children; Please note that the number of leaf nodes is not power of 2. Therefore, you may need to change the way in which intermediate nodes are calculated. There are different ways to handle this. Please label clearly how you calculate each node.
   2. Now the creator of the file F6 needs to verify that his file’s hash value is integrated in the root of the tree. Please show the minimum number of hash values in the tree that the creator needs to accomplish the task. Please also show how the verification is accomplished.