DFSC1316: Digital Forensic and Information Assurance I

Assignment 2 (Due Tue, 10/24/2017 23:59:99)

Rules:

1. All you answers will be typed unless otherwise being advised.
2. Submit you assignment in PDF version (Office word can be directly saved as PDF, or you can use virtual PDF printer to 'print' it as pdf).

---

1. **(25pts) What is the main difference between secret key cryptography algorithm and public key cryptography algorithm? Explain why secret key algorithm does not support non-repudiation, and how can public key algorithm support it.**
   Secret keys are also known as symmetric cryptography keys. Their strength lie in the key itself. Both the sender and receiver have identical keys. With public keys, the encryption key is public, but the decryption key is private. Since both parties share the same key, it cannot be determined who was the source. Public key cryptography solves this by having only the receiver's private key be able to decrypt the message.

2. **(25pts) Explain how to implementation authentication between Alice and Bob, using secret key, public key, and Hash algorithms.**
   With a secret key, the same key is shared between both Alice, and Bob. This is then used to encrypt and decrypt the message.
   With a public key, Alice uses her public key to encrypt the message, and Bob can use his private key to decrypt the message.
   Hash algorithms can only be computed one way. If you can hash a file and you get the same hash, it is authentic.

3. **(25pts) Why it is so important that we require it is difficult to find two messages with the same message digest?**
   The harder it is to create a collision, the more secure and harder it is to falsify. This provides a great deal of authenticity to the content.

4. **(25pts) Bob obtained a forensics copy (that is, an image) of a hard drive from a crime scene. He runs a Hash algorithm to compute the Hash of the image, and stores the Hash value along with the image on a portable hard drive, which is then taken care of by Trudy.**
   After some time, when Bob get the hard drive back from Trudy, he suspect that Trudy may have changed the content of the forensics image.
   Therefore, Bob run the same Hash algorithm again with the image on the hard drive, and found that the Hash value matches what was stored on the hard drive.

Question: is this an indication that Trudy has not done anything to the image? Why or why not?

This would indicate that, unless the hash stored on the drive has been altered, the data has not been tampered with. Because of the nature of a hashing function, a slight difference in data would result in a completely different hash digest.