IT IS 3200

Homework 1

Total marks: 30

Roman Styrku

Due: 9/12/2018

1. Most of you use social media regularly. Describe any two attacks associated with it. (4 pts)

- Two social media attacks are Phishing (Trying to get your login information by pretending to be the Social Media site) and Fake profiles (Creating a profile and pretending to be someone else in order to get further access to the “friends” of the person the hacker is pretending to be.)

2. Smart home is going popular. Describe a recent attack briefly. (3 pts)

- In July Samsung’s Smart Home Gadgets were found under attack where hackers were getting unrequested access to the gadgets.

3. What are the differences between assurance and evaluation in computer security strategy. (3 pts)

- Assurance is when you are sure of the security of the technological device you are dealing with. Evaluation is when you are not sure that it is secure but you are constantly evaluating it to make sure unauthorized access isn’t granted.

4. Classify the following attacks in terms of passive attack or active attack or both. Justify your answer: (4 pts)

a. Ransomeware - Active

b. Phishing and Whaling attack - Passive

5. What is the importance of standards in security. (2 pts)

- Standards are important to know what needs to be looked after more. If you have information that needs to be kept more secure you will use the standards to decide how to implement the security measures for the information.

6. Why Brute-Force attack may fail against symmetric encryption. Give real world example. (2 pts)

- A reason that a Brute Force attack may fail symmetric encryption is because of how long it will take to go through all of the possible passwords. If your encryption is based on a 256bit key then it will take years if not decades to try every possible outcome and the hacker most likely won’t simply figure it out by guessing.

7. Draw a flow chart for the encryption and decryption steps of Triple DES. Describe the steps briefly.

- Encryption -> Encrypt Password -> Encrypt First Encryption -> Encrypt Second Encryption.

- Decryption -> Decrypt The Encryption -> Decrypt The Decrypted Encryption -> Decrypt Again to Find Password.

8. Describe the basic differences between block and stream ciphers . (3 pts)

- Stream Ciphers encrypt one bit at a type. Block ciphers encrypt a block of bits at a time.

9. Write down four advantages of public-key cryptosystem. (2 pts)

- More Secure Identity Checks

- More Secure Passwords

- Minimizes the need for interactive logins

- Uses more secure measures than just a simple username and password.

10. What is message authentication? How is it different from using symmetric encryption or using public-key encryption? (3pts)

- Message authentication is where a short piece of information is used to authenticate the message. This is used in order to make sure the message came from the actual sender and not a hacker.