IERG4130: Introduction to Cyber Security **Fall 2017**

Assignment 2

Deadline: HKT 17:00, Dec 4, 2017

Please answer all of the questions. Submit an A4 size hard copy to the designated homework box on or before the deadline. You are reminded that you are not allowed to copy from any sources without proper citations and acknowledgements. All submissions must include a declaration of academic honesty contained in the website http://www.cuhk.edu.hk/policy/academichonesty/.

Question 1: True or False. Explain your answer.

(1) Consider using compression in conjunction with encryption to save the storage/bandwidth requirement while offering security, one should encrypt then compress instead of compress then encrypt.

(2) To provide the same level of security, the RSA based encryption scheme uses a shorter key than the elliptic curve cryptography (ECC) based one.

(3) Retinal scanning is a very stable, effective and, secure authentication method because retina remains unchanged even in the presence of diseases and even twins do not have an identical retinal pattern.

(4) Botnets must be used for denial of service attacks.

Question 2: RSA Cryptosystem

(a) Given $N = pq = 97 \times 131 = 12707$, $\mathsf{ek} = 8383$. Find the value of the Euler's totient evaluated at N, and hence the decryption key dk of the RSA encryption scheme. Show your steps.

(b) Decrypt $c = 2017$ by Chinese Remainder Theorem (CRT) and repeated squaring. Show your steps.

Question 3: Diffie-Hellman Key Exchange Protocol

Suppose Alice, Bob and Carol with public keys g^a, g^b, g^c respectively (with a, b, c being the private keys and g being a public generator) want to come up with a shared key g^{abc}. Assume they know each others public key.

(a) Propose a key exchange protocol (i.e., show the steps each party needs to do including both their local computation and their preparation of messages for interaction) that is secure such that an eavesdropper David cannot learn the shared key g^{abc} by looking at the protocol messages.

(b) Why David cannot learn the shared key g^{abc} by looking at the protocol messages when the protocol you proposed in a) is used? What assumption is the protocol relying on? Briefly state the assumption.

Question 4: Needham-Schroeder Protocol

(a) What is replay attack? How can Needham-Schroeder Protocol prevent against replay attack?

(b) What is CIA triad? Which part(s) of CIA triad is(/are) replay attack violating? Explain.

Question 5: Network Security

Which of the following capabilities, eavesdrop, inject packets (with forged source address), modify packets or drop packets are required to perform the following attacks? (a) DNS spoofing, (b) TCP SYN flood, (c) Smurf amplification, (d) TCP session hijacking. Note that some of the attacks may require none of the capabilities.