Beijing-Dublin International College

SEMESTER I FINAL EXAMINATION - 2017/2018

School of Software Engineering

COMP3031J Security and Privacy

HEAD OF SCHOOL NAME: Qing Zhu
MODULE COORDINATOR NAME: Jingsha He
OTHER EXAMINER NAME: Xiang Li

Time Allowed: 90 minutes

Instructions for Candidates

BJUT Student ID: _____ **UCD Student ID:** _____

I have read and clearly understand the Examination Rules of both Beijing University of Technology and University College Dublin. I am aware of the Punishment for Violating the Rules of Beijing University of Technology and/or University College Dublin. I hereby promise to abide by the relevant rules and regulations by not giving or receiving any help during the exam. If caught violating the rules, I accept the punishment thereof.

Honesty Pledge: _____ **(Signature)**

Instructions for Invigilators

Non-programmable calculators are permitted.
No rough-work paper is to be provided for candidates.

Obtained score

Question 1: 15 True/False questions (2 points for each question, 30 points in total). Please select ONLY ONE of the two choices.

1. The realistic goal of information security is to make it more costly to perform unauthorized access to information than the value of the information.
   (1) True (2) False
2. CBC (cipher block chaining) mode in DES/AES would make successful decryption of a cipher block dependent on that of all preceding cipher blocks.
   (1) True (2) False
3. In a symmetric cryptosystem in which both the sender and the receiver use a shared secret key to conduct secure communication, the receiver is able to prove that a message is indeed sent by the sender.
   (1) True (2) False
4. In an asymmetric cryptosystem, a sender would use his/her own public key to encrypt a message before sending it to a receiver to ensure the confidentiality/secrecy of the message.
   (1) True (2) False
5. Kerberos is a network authentication protocol based on public key cryptography.
   (1) True (2) False
6. The strength of an encryption algorithm should rely on how well the details of the algorithm is protected from being disclosed to the general public.
   (1) True (2) False
7. Access control matrix is considered to be a model for information security because it can describe who can access what regardless of the numbers of subjects, objects and access rights.
   (1) True (2) False
8. Triple-DES is stronger than DES because it uses a single key of three times in length compared to the key used in DES.
   (1) True (2) False
9. Single sign-on (SSO) provided by Kerberos authentication allows the user to use a single password to successfully authenticate to multiple application servers.
   (1) True (2) False
10. In a public key cryptosystem in which $USER_{PK}$ and $USER_{SK}$ are USER's public and private keys, respectively, then $Bob_{PK}(Bob_{SK}(M))=Bob_{SK}(Bob_{PK}(M))$.
    (1) True (2) False

11. Mandatory security rules takes a higher priority than discretionary security rules for access control to protect information in the Bell-LaPadula Model.

    (1) True (2) False

12. A random number could be included in messages in the protocol design to equip the protocol with the capability of countering reply attacks.

    (1) True (2) False

13. Storing the hash value of a password on the server is believed to be a more secured way of protecting the password.

    (1) True (2) False

14. A certificate authority can be used to bind a user identity to a shared secret key in a secret key based crypto-infrastructure.

    (1) True (2) False

15. An access control list (ACL) can be made shorter after applying the default rule of "no access" when there is no access right explicitly specified in the list for a subject.

    (1) True (2) False

Obtained score

Question 2: Concept questions (5 points for each question, 30 points in total).

1. List the three main issues that computer security is concerned about and discuss the consequences resulting from the violation of the respective requirements.
2. Explain what the RSA algorithm is designed for and why public key based encryption consumes more time in general than secret key based encryption using algorithms such as the AES when they are applied to the same plain text.
3. Explain what message digest is and why it can generally help to reduce the computational overhead for the authentication of messages.
4. Explain the purpose of the Bell-LaPadula model and the implications of enforcing the two access checks in the mandatory part of access control in the model.
5. Describe how the use of certificates can resolve the trust issue associated with identities (IDs).
6. Explain what the "least privilege" principle is and describe the temporal and spatial requirements that accompany this principle.

Obtained score

Question 3: General question (10 points).

1. Explain why public key cryptography can support the authentication of the origin of a message. (5 points)
2. Let's suppose that, in a secret key cryptosystem, Alice and Bob share a secret key. Now, Bob claims that he can prove that he received a message from Alice because he can show both the clear text and the cipher text of the message and can also prove that the clear text is decrypted from the cipher text using the secret key that they share. Explain why Bob's claim cannot satisfy the requirement for the authentication of the origin of a message. (5 points)

Obtained score

Question 4: General question (10 points).

Given the following group membership setup and the access control list (ACL) in the Windows environment, determine the access rights for Bob, Alice, John and Peter for access to file c:\document:

Manager = {Peter};

Engineer = {Bob, Alice, John, Peter};

ACL(c:\document) = {(Manager, {own}), (Engineer, {read, write}), (John, {no access})}.

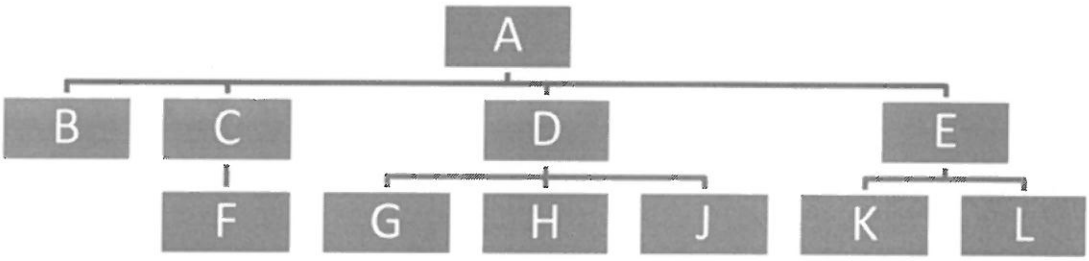
Obtained score

Question 5: General question (10 points).

1. Describe what network single sign-on tries to achieve. (5 points)
2. Describe how Kerberos authentication protocol works to achieve network single sign-on in which you should specifically describe how "Ticket" and "Authenticator" should be constructed. (5 points)

Obtained score

Question 6: General question (10 points).



In a public key infrastructure (PKI) such as the one shown above, a node can accept the public key of another if and only if the public key is certified by the certificate authority (CA) that the node trusts and uses. Such a trust relationship can be expressed with a parent-child relationship between a CA and its children nodes in the PKI. Thus, a parent node in such a PKI is the CA for all of its children nodes. Answer the following questions based on the above PKI:

1. Explain how a CA (the parent) certifies the public key of a child node. (2 points)
2. Describe a procedure for node K to get the public key of node L. (3 points)
3. Describe a procedure for node F to get the public key of node H. (5 points)