Beijing-Dublin International College

SEMESTER I FINAL EXAMINATION - 2019/2020

Faculty of Information Technology

COMP3031J Security and Privacy

HEAD OF SCHOOL NAME: Junfei Qiao
MODULE COORDINATOR NAME: Jingsha He
OTHER EXAMINER NAME:

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 unauthorized access to information more costly than the value of the information rather than to protect information at any cost.
   (1) True (2) False
   True. 1-Overview中指出安全目标是保护成本不应超过资产价值，攻击代价应高于资产价值

2. The purpose of the CBC (cipher block chaining) mode in DES is to improve the performance of DES encryption and decryption.
   (1) True (2) False
   False. 2-Crypotography中指出CBC块依赖于前一个密文块; 没有直接提到性能，但是从原理上讲，CBC模式由于存在依赖关系，无法进行并行处理，因此速度通常慢于ECB模式。

3. In a symmetric cryptosystem in which both the sender and the receiver use a shared secret key to conduct secure communication, the receiver has all it needs to prove that a message is indeed sent by the sender.
   (1) True (2) False
   False. 2-Crypotography 中 对称加密使用的是单一共享密钥。在对称加密中，密钥是共享的。接收方自己也可以伪造一条消息声称是发送方的。因此，仅靠对称加密，接收方无法向第三方证明消息是发送方发送的。

4. In an asymmetric cryptosystem, a sender can use anyone's public key to encrypt a message before sending it to a receiver to achieve the confidentiality of the message with the receiver.
   (1) True (2) False
   False. 2-Cryptography. 发送方必须使用接收方的公钥进行加密。

5. Kerberos is a network authentication protocol based on secret key cryptography.
   (1) True (2) False
   True.

6. It is generally agreed that the strength of an encryption algorithm should mainly rely on the secrecy of the algorithm.
   (1) True (2) False
   False. 2-Cryptography. 算法应公开，安全强度应仅依赖于密钥.

7. The reason why access control matrix is regarded as a model for information security is because it can describe who can access what regardless of the numbers of subjects, objects and access rights.
   (1) True (2) False
   True. 3-Security.

8. Triple-DES is stronger than DES because it uses a single key that is 3 times in length of the key that is used in DES to perform encryption.
   (1) True (2) False
   False. 2-Cryptography. 使用3个密钥进行三次加密操作。

9. Kerberos requires that the same password be presented by the user to successfully authenticate to each of the application servers.
   (1) True (2) False
   False. 4- Identification中,kerberos是单点登录，用户只需向认证服务器认证一次，后续无需认证。

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
    True.

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

(1) True (2) False

True. 3-Security. 在Bell-LaPadula模型中，强制安全规则（MAC）在保护信息的访问控制方面总是比自主安全规则（DAC）具有更高的优先级。

12. Including a random number in a message is a common mechanism for making a protocol capable of dealing with reply attacks.

True.

(1) True (2) False

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

True

(1) True (2) False

14. Certificate can be used as a mechanism for binding a user identity to a shared secret key for key exchange in a secret key based crypto-infrastructure.

(1) True (2) False

False. 2-Cryptography. 证书是将共钥与用户身份绑定的令牌。对称加密系统中，不可能将密钥与身份绑定，因为密钥是共享的。a

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

(1) True (2) False

True。5-Access.
Slide 7 提到了 "Principle 2: Fail-Safe"（故障安全原则）： "The default access right... should be 'no access'"
Slide 19 关于 ACL 的 "Default permissions"： "Access request... is denied if the subject doesn't appear in the ACL"
如果不采用默认拒绝规则，你需要显式地列出所有不能访问该文件的用户（黑名单），这在用户众多的系统中会导致列表极其庞大。采用默认拒绝（白名单机制）后，只需列出有权限的少数用户，从而缩短列表。

Obtained score

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

1. Confidentiality: Unauthorized disclosure of information. Leads to theft of information or loss of privacy.
Integrity: Unauthorized modification of information. Leads to damage to information or theft of money.
Availability: Unauthorized inhibition of access to information by authorized users. Leads to disruption of service.

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 encrypting the same plain text.

RSA is designed for Public Key Cryptography. RSA relies on complex matmatical calculations, whereas like AES use fast bit-oriented operations.

3. Explain what message digest is, how it is generally obtained and why it can generally help to reduce the computational overhead of message authentication.
4. Explain what the Bell-LaPadula model is as well as the implication of enforcing the two access checks in the mandatory control of the model.
5. Describe how the use of certificate can help resolve the trust issue associated with identities (IDs).
6. Explain what the “least privilege” principle means and describe the temporal and spatial requirements implied by this principle.

3. message disest is an output of a fixed size produced from an input mesage of any length. Compute using a cryptographic has function. Instead of encrypting the entire large message, the system only encrypts the small, fixed-size message digest.

4.It is a confidentiality policy model based on military security classifications. No Read Up; No write Down. Ensure taht information is never allowed to flow downwards.

5. A certificate acts as a token that binds a public key to an identity. CA sign each certifacation through its private key. By verifying the signature, user decryption through CA public key.

6. Need to know rule. A subject shoulf be given only those privileges that are absolutely necessary for it to complete its tasks.
Spatial Requirement: grant the privileges that are absolutely needed.
Temporal: grant the privileges only when it is absolutely need.

Obtained score

Question 3: General question (10 points).

1. Explain why public key cryptography can support non-repudiation of the origin of a message. (5 points)

   Because only the sender controls the private key, and anyone can verify using the sender's public key, the sender can not falsely deny having sent the message.

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 authentication of the origin of a message. (5 points)

   Bob himself or anyone with the shared key could have generated the same ciphertext. There is no third-party verifiable proof of origin.

Obtained score

Question 4: General question (10 points).

RSA algorithm can be used to generate a private-public key pair. The key generation formula in the Diffie-Hellman key exchange algorithm can also be used to compute a public key from a private key. The question now is whether the Diffie-Hellman key pair can be used to perform data encryption and decryption in the same way as the RSA key pair can? Prove or disprove your answer.

No.
DH is for key exchange, not direct encryption. To encrypt data, DH is used to first derive a session key, then encrypt data with a secret-key algo. using that session key.

Obtained score

Question 5: General question (10 points).

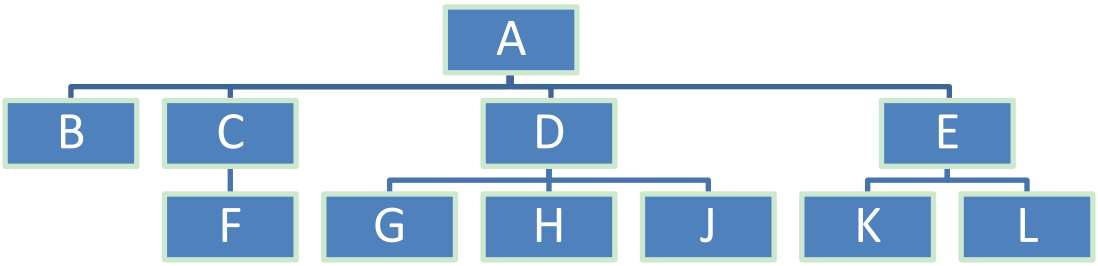
SSO allows a user to authenticate only once with Authentication Server(AS). After this initial authentication, the user can access multiple application servers without being asked to entire their passward.

1. Describe what network single sign-on is. (5 points)
2. Describe how the Kerberos authentication protocol works to achieve network single sign-on in which you should focus on describing the general principle of constructing the "Ticket" and the "Authenticator". (5 points)

   Ticket is encrypted using Server's secret key. Contains the Seesion Key, Client Identity and validity period.
   Authenticator is encrypted using the Session Key. Contains Client Identity and a Timestamo.

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 node if and only if the public key is certified in the form of a certificate by the same certificate authority (CA) that can certify the public key of the first node. This is possible due to the fact that both nodes have the public key of the CA. This certificate issuing structure can be expressed using 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 certifies the public key of a child node. (2 points)
2. Describe a procedure for node G to obtain the public key of node H. (3 points)
3. Describe a procedure for node F to obtain the public key of node L. (5 points)

1. CA issues a certificate that binds an identity to a public key. CA signs the certificate by encrypting with private key. Anyone who has CA's public key can verify the certificate by decrypting.

2. G gets H's certificate signed by D. G verifies it using D's public key, checks timestamp, and extracts P_H

3. C verifies **E's certificate** using **A's public key**

C verifies **L's certificate** using P_E and gets P_L.

C **re-certifies** P_L by issuing a new certificate for L **signed by C**

F verifies this new certificate with P_C and obtains P_L