= 3 = +

z

eso

a i

Beijing-Dublin International College

SEMESTER | 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:

| have read and clearly understand the Examination Rules of both Beijing University of Technology and University College Dublin. | am aware of the Punishment for Violating the Rules of Beijing University of Technology and/or University College Dublin. | 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, | 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. BDIC Semester One Academic Year (2017-2018)

Obtained | Question 1: 15 True/False questions (2 points for each question, 30 points in total).

score | Please select ONLY ONE of the two choices.

The realistic goal of information security is to make it more costly to perform unauthorized access to information than the value of the information. **T**

1. True (2) False

CBC (cipher block chaining) mode in DES/AES would make successful decryption of a cipher block dependent on that of all preceding cipher blocks. **T**

1. True (2) False

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. **F**

1. True (2) False

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. **F**

1. True (2) False

Kerberos is a network authentication protocol based on public key cryptography. **F**

1. True (2) False

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. **F**

1. True (2) False

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. **T**

1. True (2) False

Triple-DES is stronger than DES because it uses a single key of three times in length compared to the key used in DES. **F**

1. True (2) False

Single sign-on (SSO) provided by Kerberos authentication allows the user to use a single password to successfully authenticate to multiple application servers. **T**

1. True (2) False

In a public key cryptosystem in which USERpx and USERsx are USER’s public and private keys, respectively, then Bobpx(Bobsx(M))=Bobsx(Bobpx(M)). **T**

1. True (2) False

Page 2 of 5 Tt.

BDIC Semester One Academic Year (2017-2018)

Mandatory security rules takes a higher priority than discretionary security rules for access controlto protect information in the Bell-LaPadula Model. **T** (1) True (2) False

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

(1) True (2) False

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

1. True (2) False

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

1. True (2) False

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. **T**

(1) True (2) False

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

score

List the three main issues that computer security is concerned about and discuss the consequences resulting from the violation of the respective requirements.

* 1. **Confidentiality: The secrecy and privacy information such as your personal information will be read by unauthorized entity, and they may publish in the network to defame you.**
  2. **Integrity: The information is modified by unauthorized entity, so you get wrong information.**
  3. **Availability: The information is not available for you due the inhibition of access to the information such as DoS(denial of service), so you can’t get what you what.**

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.

1. **RSA algorithm is designed for transmitting sensitive information over a network.**
2. **RSA generally deals with large exponents in its encryption process according to formula: c=m^p mod n or c=m^s mode n, which is the root cause of the inefficiency. While for AES, the operations like transposition and substitution are not too time consuming.**

Explain what message digest is and why it can generally help to reduce the computational overhead for the authentication of messages.

1. **Message digest is a kind of process which convert any length of input to a small fixed length output using a hash function which normally reduce the length of message.**
2. **The main reason it can help to reduce the computational overhead is because of the short message it returns, and the encryption and decryption process of public key-based cryptography is inefficient when dealing with long length messages.**

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.

1. **The purpose of the Bell-LaPadula model is to create a confidentiality model which can avoid the unauthorized disclosure of information.**
2. **Implications of enforcing the two acces checks in the mandatory part of access control: Information can only flow UPWARDS**

Describe how the use of certificates can resolve the trust issue associated with identities (IDs).

1. **The certificate should be signed by a certificate authority(CA) and encryption with CA’s private key. The trustfulness of certificate depends on how much the user trust the CA.**
2. **The user gets certificates and verify a certificate through decryption with CA’s public key and retrieve the public keys and identities from certificate.**

Explain what the “least privilege” principle is and describe the temporal and spatial requirements that accompany this principle.

1. **A subject should be given the privileges that are absolutely necessary for the subject to complete its tasks or functions, which means a subject should not be given the privileges that it does not need.**
2. **Spatia requirements: grant the privileges that are absolutely needed(in space)**
3. **Temporal requirements: grant the privileges only when it is absolutely needed(in time)**

Page 3 of 5 BDIC Semester One Academic Year (2017-2018)

Obtained | Question 3: General question (10 points).

score

1. Explain why public key cryptography can support the authentication of the origin of a message. (5 points)
2. **The reason is that the message can be encrypted with private key of the sender as the private key is only known to sender nobody else can get the private key.**
3. **Then when the cipher is sent to receiver, the message can be decrypted by public key of sender which can be known by anyone, so if the receiver can get the message, then it can make sure the message is sent from the sender.**
4. 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)
5. **The Bob need to verify the identity of message if it is really sent from Alice which can not achieved through secret key cryptosystem. Because Bob can not check the identity of message through shared key.**
6. **The message received by Bob may not come from Alice. It may under a replay attack by someone else who have got their history messages and then sent to Bob as he/she is Alice.**

Obtained | Question 4: General question (10 points). score

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::

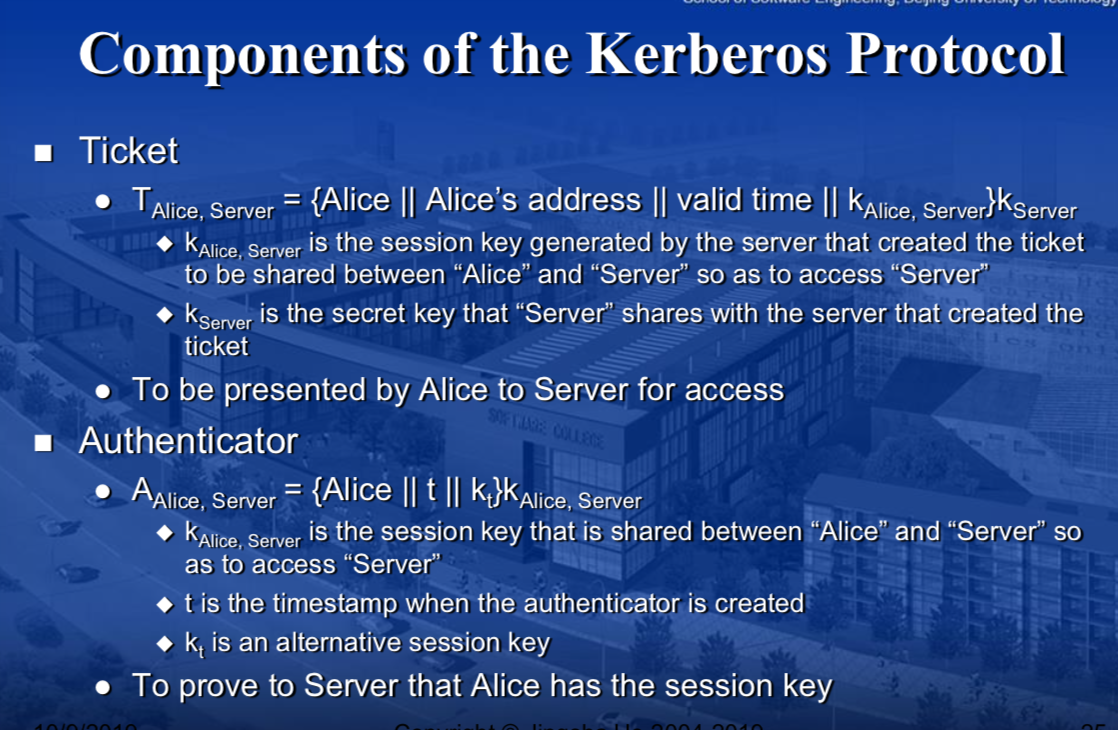
Manager = {Peter}; Engineer = {Bob, Alice, John, Peter};

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

1. **Bob, Alice: read and write**
2. **John: no access**
3. **Peter: read, write, own**

Obtained | Question 5: General question (10 points). score

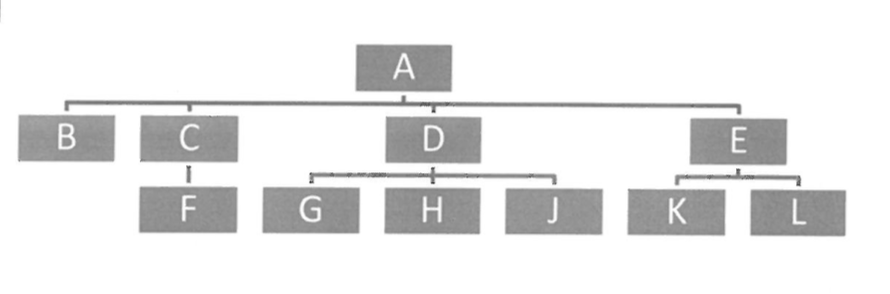
1. Describe what network single sign-on tries to achieve. (5 points)
2. **The single sign-on tries to achieve that user only needs to log in once with the Authentication Server (AS) and Ticket-Granting Server(TS) issues tickets to the user to access the application servers.**
3. **So the user can log in any application servers which is connected to the AS with the tickets issued by TS and the log in process is actually transparent to the user.**
4. 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)

**1.** 

Page 4 of 5 BDIC Semester One Academic Year (2017-2018)

Obtained | Question 6: General question (10 points). score

7 2



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)

**CA encrypt the public key and identity of a child node with its private key, so the child node can decrypt the certificate with the public key of CA.**

1. Describe a procedure for node K to get the public key of node L. (3 points)

**Node K get certificate of node L from node L, and then decrypt this certificate with the public key of E and get the public key of node L.**

1. Describe a procedure for node F to get the public key of node H. (5 points)

**Node F get certificate of node H which is issued by node D, so node C need to convert this certificate to become a certificate that is issued by node C as Node F only has the public key of node C. Node C need to get public key of Node D from Node A first, and then decrypt the certificate issued by node D with this public key and encrypt the public key of node H with the private key of node C.**