Vietnam National University, Hanoi
University of Engineering and Technology

Faculty of Information Technology
2020

Duration : 120 minutes
Class : INT3307

Open books and notes, no notebooks, no mobile phones
No discussion or exchange of documents between students during the exam

Final Exam
Network Security

(4 problems, 3 pages, point values given in parentheses, 10 maximum)

1. Kerberos 4 (2.5 points)

Write an authentication dialogue that satisfies the same requirements and follows the same steps as the following dialogue.

- **Once per user logon session**

  (1) C → AS: $ID_c \parallel ID_{tgs}$

  (2) AS → C: E(K_c, $Ticket_{tgs}$)

- **Once per type of service**

  (3) C → TGS: $ID_c \parallel ID_v \parallel Ticket_{tgs}$

  (4) TGS → C: $Ticket_v$

- **Once per service session**

  (5) C → V: $ID_c \parallel Ticket_v$

$Ticket_{tgs}$ = E(K_{tgs}, [$ID_c \parallel AD_c \parallel ID_{tgs} \parallel TS_1 \parallel Lifetime_1$])

$Ticket_v$ = E(K_v, [$ID_c \parallel AD_c \parallel ID_v \parallel TS_2 \parallel Lifetime_2$])

The new authentication dialogue has to use public-key cryptography instead of symmetric encryption, i.e.

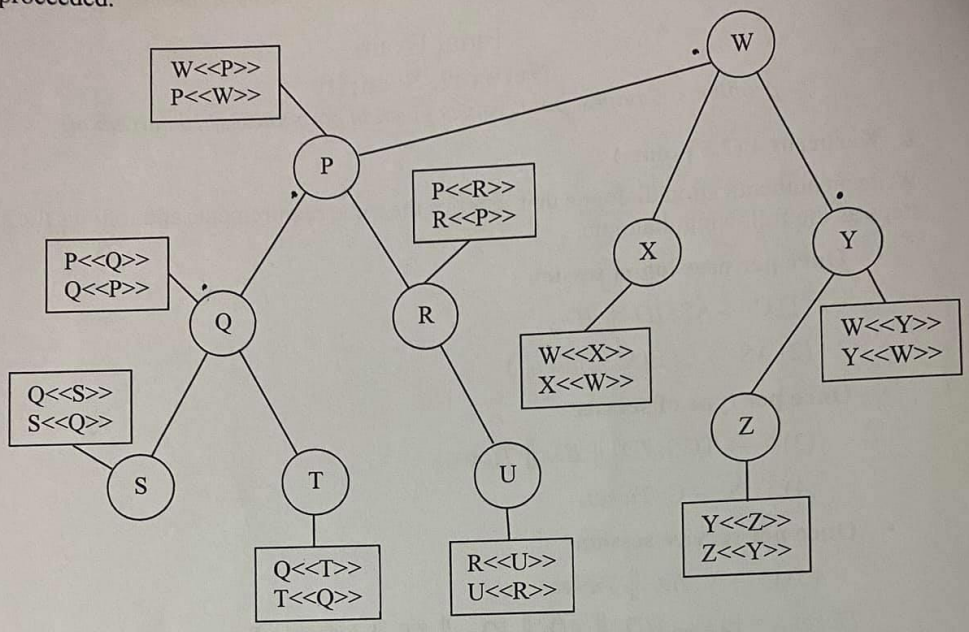
- The authentication server AS, the ticket granting server TGS, the user ID_c, and the service server V, each has a RSA public key certified by a same certificate authority named CA, which can be used for both digital signature and encryption purposes
- Initially, AS has the public key certificate CA<<ID_c>> of each user ID_c, AS has the public key certificate CA<<TGS>> of TGS, TGS has the public key certificates CA<<AS>> of AS and CA<<V>> of each service server V, each service server V has the public key certificate CA<<TGS>> of TGS
- Each user ID_c doesn't have a password P_c stored in the form of the corresponding hash value P_c on the authentication server AS as in Kerberos 4
- The authentication server AS doesn't have a common secret key K_{tgs} shared with the ticket granting server TGS as in Kerberos 4
- The ticket granting server TGS doesn't have a common secret key K_v shared with each service server V as in Kerberos 4

2. X.509 certificates (2.5 points)

Consider the X.509 hierarchy in the next page.

Suppose that user A has obtained a certificate from certification authority Q and user B has obtained a certificate from certificate authority Y. Give the chain of certificates that allows

A to verify that the certificate of B issued by Y is valid. Explain how the verification is proceeded.



3. Transport-level security (2.5 points)

Consider the SSL Handshake Protocol. Suppose that the RSA key exchange method is used. Both the client and the server have a fixed RSA public/private key pair. Both public keys are certified by a certificate authority. They can only be used for digital signature purposes and are not suitable for encryption. The client and the server need to authenticate each other.

a. (1 point)

Draw the message exchange expected for this scenario.

b. (1.5 point)

Describe the parameters associated with each situation dependent message and with the *client_key_exchange* message.

4. Electronic mail security (2.5 points)

A user A maintains a PGP public key ring with the fields **Public Key**, **User ID**, **Owner Trust**, and **Signatures** as follows:

Public Key	PU_A	PU_B	PU_C	PU_D	PU_E	PU_F	PU_G	PU_H	PU_I
User ID	A	B	C	D	E	F	G	H	I
Owner Trust	*Ultimate*	*Always trusted*	*Always trusted*	*Always trusted*	*Usually trusted*	*Usually trusted*	*Usually trusted*	*Untrusted*	*Unknown*
Signatures	-	A, K	E, F	E, J	B, F	A, B	D, E	C, D	D, H

The **Key Legitimacy** fields are computed on the basis of the attached signatures as follows:

- If the owner is A then the public key is *legitimate*.
- If at least one signature has a signature trust value of *ultimate*, then the public key is *legitimate*.
- Otherwise, PGP computes a weighted sum of the trust values. A weight of 1 is given to signatures that are *always trusted* and ½ to signatures that are *usually trusted*. When the total of weights of the introducers of a **Public Key/User ID** combination reaches 1, the public key is considered *legitimate*.
- In all remaining cases, the public key is considered *illegitimate*.

Draw the corresponding PGP trust model.