Duration : 120 minutes *Open books and notes, no notebooks, no mobile phones*

Class : INT3093 *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. **Key distribution and user authentication (2 points)**

Assume an open distributed environment in which users at client workstations wish to access services on servers distributed throughout the network. We would like for servers to be able to restrict access to authorized users and to be able to authenticate requests for service. Rather than building in elaborate authentication protocols at each server, an authentication server (AS) and a ticket-granting server (TGS) are used. The AS knows the passwords of all users and stores these in a centralized database. Its function is to authenticate users to servers. The TGS knows if a user can access a particular service. Consider the following hypothetical dialogue.

(i) Once per user logon session

(1) C → AS : *IDC* ║ *IDtgs*

(2) AS → C : E*KC*[*Tickettgs*]

(ii) Once per type of service

(3) C → TGS : *IDC* ║ *IDV* ║ *Tickettgs*

(4) TGS → C : *TicketV*

(iii) Once per service session

(5) C → V : *IDC* ║ *TicketV*

*Tickettgs* = E*Ktgs*[*IDC* ║ *ADC* ║ *IDtgs* ║ *TS*1 ║ *Lifetime*1]

*TicketV* = E*KV*[*IDC* ║ *ADC* ║ *IDV* ║ *TS*2 ║ *Lifetime*2]

where, C is a client workstation, *IDC* is the identifier of user on C, *IDtgs* is the identifier of TGS, V is a service server, *IDV* is the identifier of V, *Tickettgs* is the ticket to be used by client to access TGS, *TicketV* is the ticket to be used by client to access server V, *ADC* is the network address of C, *KC* is a key derived from the user’s password, *Ktgs* is a secret key known only to AS and TGS, *KV* is a secret key known only to TGS and V, *TS*1 indicates the time at which *Tickettgs* is issued, *TS*2 indicates the time at which *TicketV* is issued, *Lifetime*1 và *Lifetime*2 indicate the length of time for which the corresponding ticket is valid.

* 1. *(1 point)*

Describe two scenarios in which an opponent, without knowing the user *IDC*‘s password nor *KC*, is able to impersonate this user to obtain *TicketV* from TGS.

* 1. *(0.5 point)*

In each of the above scenarios, after obtaining obtain *TicketV* from TGS, how the opponent can do to have access to the corresponding service?

1. *(0.5 point)*

Explain how our system is vulnerable to a password attack.

1. **Transport-level security (3 points)**

Consider the SSL Handshake Protocol. Suppose that the hybrid ephemeral/fixed Diffie-Hellman key exchange method is used; the server has a fixed Diffie-Hellman public/private key pair (the Diffie-Hellman public parameters are contained in the server’s certificate); the client generates a one-time Diffie-Hellman public/private key pair but has a fixed RSA public/private key pair (the RSA public key is contained in the client’s certificate).

1. *(1.5 point)*

Draw the most secure exchange of messages expected for this scenario.

1. *(1.5 point)*

Describe the parameters associated with each situation dependent message and with the *client\_key\_exchange* message.

1. **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 |
| **User ID** | A | B | C | D | E | F | G | H |
| **Owner Trust** | *Ultimate* | *Always trusted* | *Usually trusted* | *Always trusted* | *Usually trusted* | *Usually trusted* | *Not trusted* | *Always trusted* |
| **Signatures** | - | A | A | C | C, D | B | C, F | G, I |

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.

1. **IP Security (2.5 points)**

Draw the format of the IPv4 IPSec packets as transmitted on the Internet by the security gateway GW1 of a local network LAN1 to the security gateway GW2 of another local network LAN2. Those packets have the host H1 in LAN1 as the original source and the host H2 in LAN2 as the original destination. IPSec is implemented on the devices H1, GW1, GW2, and H2. Two security association are combined together: an inner transport security association and an outer tunnel security association. In the tunnel mode, both ends of the security association are a security gateway. The inner transport security association provides data origin authentication. The outer tunnel security association provides only data confidentialy but no additional authentication

Are the given packets protected against data modification, replay and limited traffic analysis attacks? Explain why with each attack.