Faculty of Computers and Information
Assiut University
IT 422

Kerberos

1. What is the role of AS and TGS in Kerberos 4?
2. What is the difference between TGS and TGT in Kerberos 4?
3. Why does Kerberos require a loosely synchronized network?
4. Suggest a method to achieve interrealm authentication in a network with N Kerberos servers with less than N(N-1) keys.
5. Suggest a situation in which authentication forwarding is useful.
6. What is a nonce and what is the difference between it and a timestamp?
7. Kerberos 5 uses nonces. Does this mean that it needs no timestamps? Why?
8. What are the three main exchanges in Kerberos? Explain each of them briefly (no more than 2 lines each).
9. Can we use AES with Kerberos 4? Can we use it with Kerberos 5? How in each case?
10. In Kerberos 4 exchange, What happens if we do the following modifications:
    a. Remove TS_2 from message 2 (leaving it inside the ticket)
    b. Remove AD_c from *Authenticator*$_c$
    c. Replace TS_5+1 with TS_5 in message six
    d. Replace TS_5+1 with 2*TS_5 in message six
    e. Transfer $Ticket_{tgs}$ in plain in message 2
    f. Remove message 6 altogether
    g. Encrypt $Ticket_v$ with K_{tgs} rather than K_v
    h. Encrypt $Ticket_v$ with $K_{c,v}$ rather than K_v
    i. Transfer $Ticket_v$ in plain in message 4

Kerberos 4 Exchange

(1) C →AS	$ID_c \Vert ID_{tgs} \Vert TS_1$
(2) AS →C	$E(K_c,[K_{c,tgs} \Vert ID_{tgs} \Vert TS_2 \Vert Lifetime_2 \Vert Ticket_{tgs}])$
(3) C →TGS	$ID_v \Vert Ticket_{tgs} \Vert Authenticator_c$
(4) TGS→C	$E(K_{c,tgs}, [K_{c,v} \Vert ID_v \Vert TS_4 \Vert Ticket_v])$
(5) C→V	$Ticket_v \Vert Authenticator_{c2}$
(6) V →C	$E(K_{c,v}, [TS_5 + 1])$
where	$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \Vert ID_c \Vert AD_c \Vert ID_{tgs} \Vert TS_2 \Vert Lifetime_2])$ $Ticket_v = E(K_v, [K_{c,v} \Vert ID_C \Vert AD_C \Vert ID_v \Vert TS_4 \Vert Lifetime_4])$ $Authenticator_c = E(K_{c,tgs}, [ID_C \Vert AD_C \Vert TS_3])$ $Authenticator_{c2} = E(K_{c,v},[ID_c \Vert AD_C \Vert TS_5])$