KERBEROS VERSION 4

ASSIGNMENT - 3

Submitted by:
Avantika Chhabra(2015MCS2334)
Vamsi Yalavarthi(2015MCS2358)

PROBLEM STATEMENT:

- This application relates to providing a session and service ticket.
- This includes maintaining of :

  Authentication Server(AS)
  Ticket Granting Server(TGS)
  Web Server(V)
- Client makes use of tickets that are granted on request by AS and TGS to communicate with the server.

INTRODUCTION:

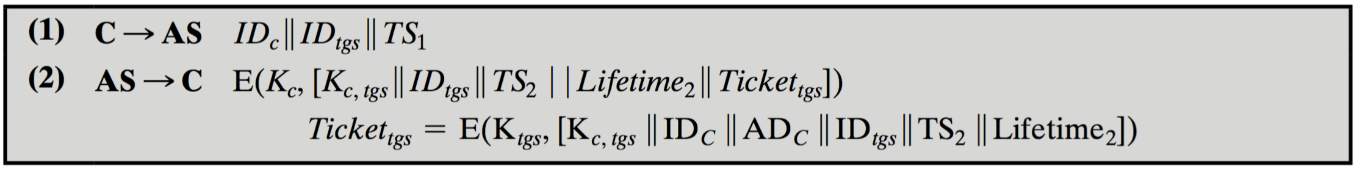
- Here a client sends his ID to AS and requests for a ticket to TGS.
- Then AS generates a ticket using a key known to both AS and TGS and sends its back to client.
- Client then contacts TGS for a ticket to access Server.
- TGS generates a ticket for each request and then sends to client.
- Client can get service using that ticket form the web server.

SOFTWARE MODULES:

There are basically three different modules.

1. Server Module
2. Ticket Granting Server Module
3. Authentication Server Module

AUTHENTICATION SERVER:



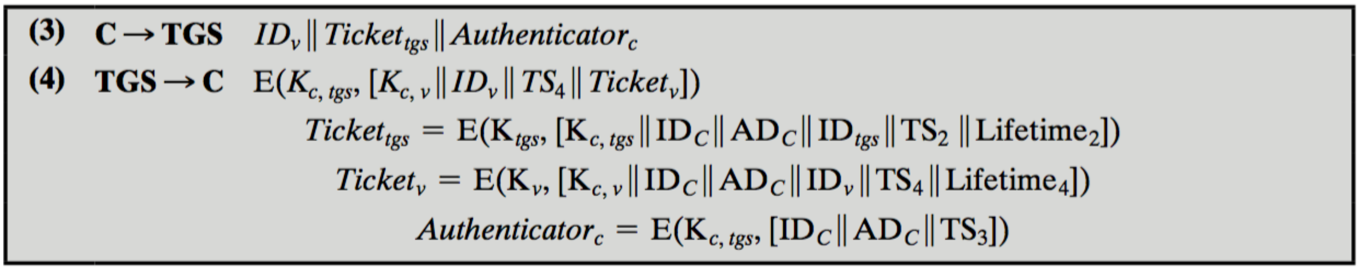
(1) **C → AS** $ID_c \| ID_{tgs} \| TS_1$

(2) **AS → C** $E(K_c, [K_{c,\,tgs} \| ID_{tgs} \| TS_2 \; | \, | \; Lifetime_2 \| Ticket_{tgs}])$

$$Ticket_{tgs} = \mathrm{E}(\mathrm{K}_{tgs}, [\mathrm{K}_{c,\,tgs} \| \mathrm{ID}_C \| \mathrm{AD}_C \| \mathrm{ID}_{tgs} \| \mathrm{TS}_2 \| \mathrm{Lifetime}_2])$$

(a) Authentication Service Exchange to obtain ticket-granting ticket

TICKET GRANTING SERVER:



(3) **C → TGS** $ID_v \| Ticket_{tgs} \| Authenticator_c$

(4) **TGS → C** $E(K_{c,\,tgs}, [K_{c,\,v} \| ID_v \| TS_4 \| Ticket_v])$

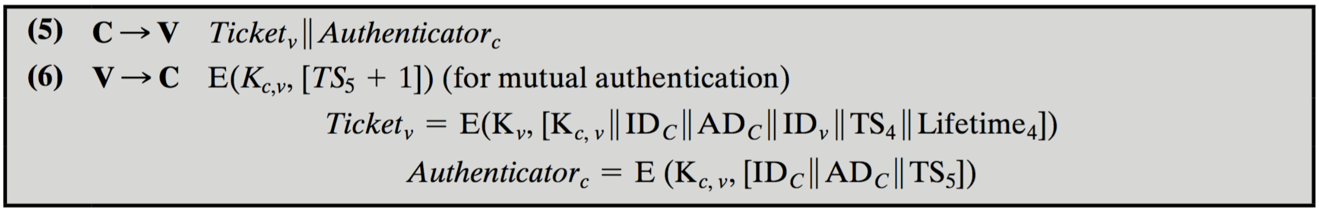
$$Ticket_{tgs} = \mathrm{E}(\mathrm{K}_{tgs}, [\mathrm{K}_{c,\,tgs} \| \mathrm{ID}_C \| \mathrm{AD}_C \| \mathrm{ID}_{tgs} \| \mathrm{TS}_2 \| \mathrm{Lifetime}_2])$$

$$Ticket_v = \mathrm{E}(\mathrm{K}_v, [\mathrm{K}_{c,\,v} \| \mathrm{ID}_C \| \mathrm{AD}_C \| \mathrm{ID}_v \| \mathrm{TS}_4 \| \mathrm{Lifetime}_4])$$

$$Authenticator_c = \mathrm{E}(\mathrm{K}_{c,\,tgs}, [\mathrm{ID}_C \| \mathrm{AD}_C \| \mathrm{TS}_3])$$

(b) Ticket-Granting Service Exchange to obtain service-granting ticket

WEB SERVER:



(5) **C → V** $Ticket_v \| Authenticator_c$

(6) **V → C** $E(K_{c,v}, [TS_5 + 1])$ (for mutual authentication)

$$Ticket_v = \mathrm{E}(\mathrm{K}_v, [\mathrm{K}_{c,\,v} \| \mathrm{ID}_C \| \mathrm{AD}_C \| \mathrm{ID}_v \| \mathrm{TS}_4 \| \mathrm{Lifetime}_4])$$

$$Authenticator_c = \mathrm{E}\ (\mathrm{K}_{c,\,v}, [\mathrm{ID}_C \| \mathrm{AD}_C \| \mathrm{TS}_5])$$

(c) Client/Server Authentication Exchange to obtain service

OVERVIEW:

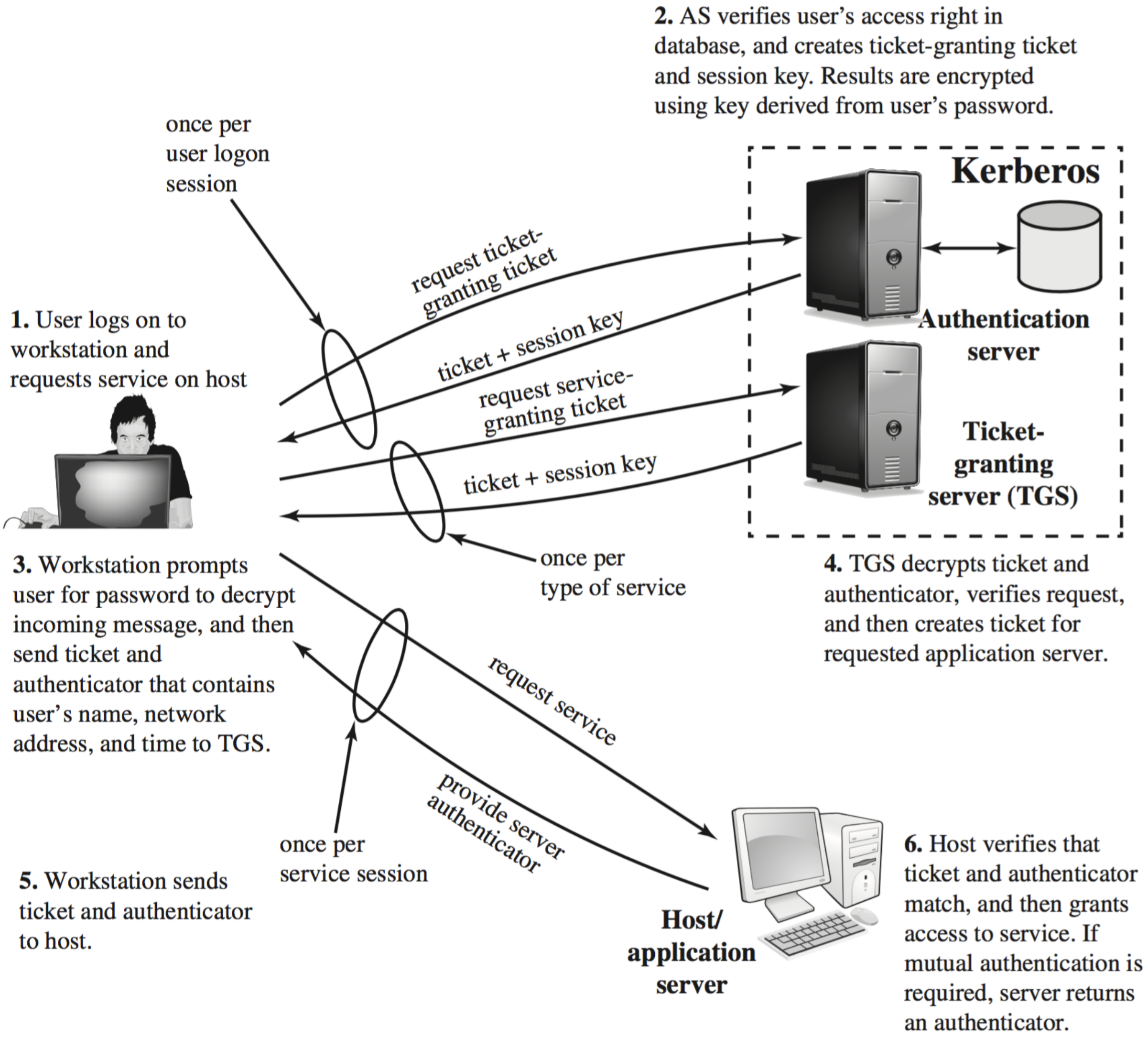
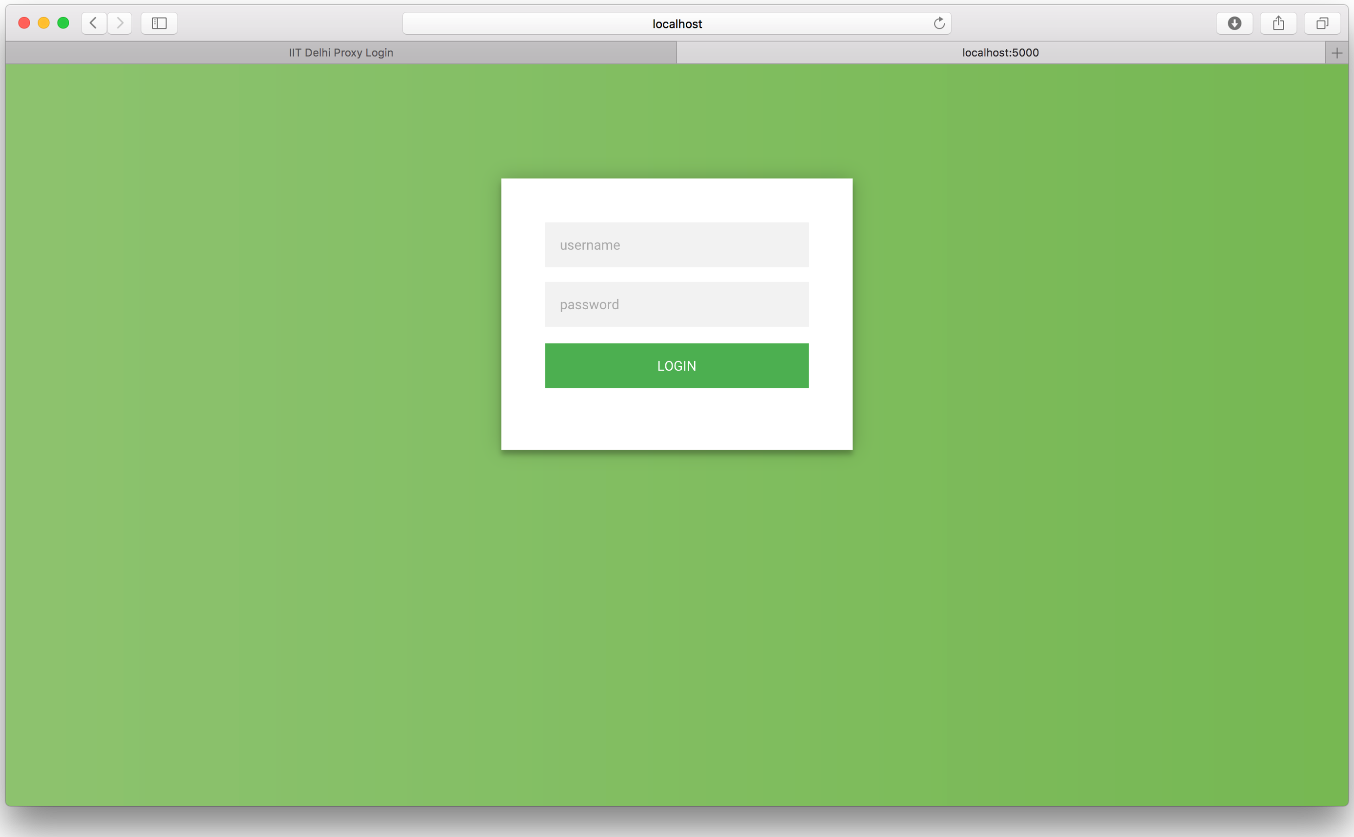
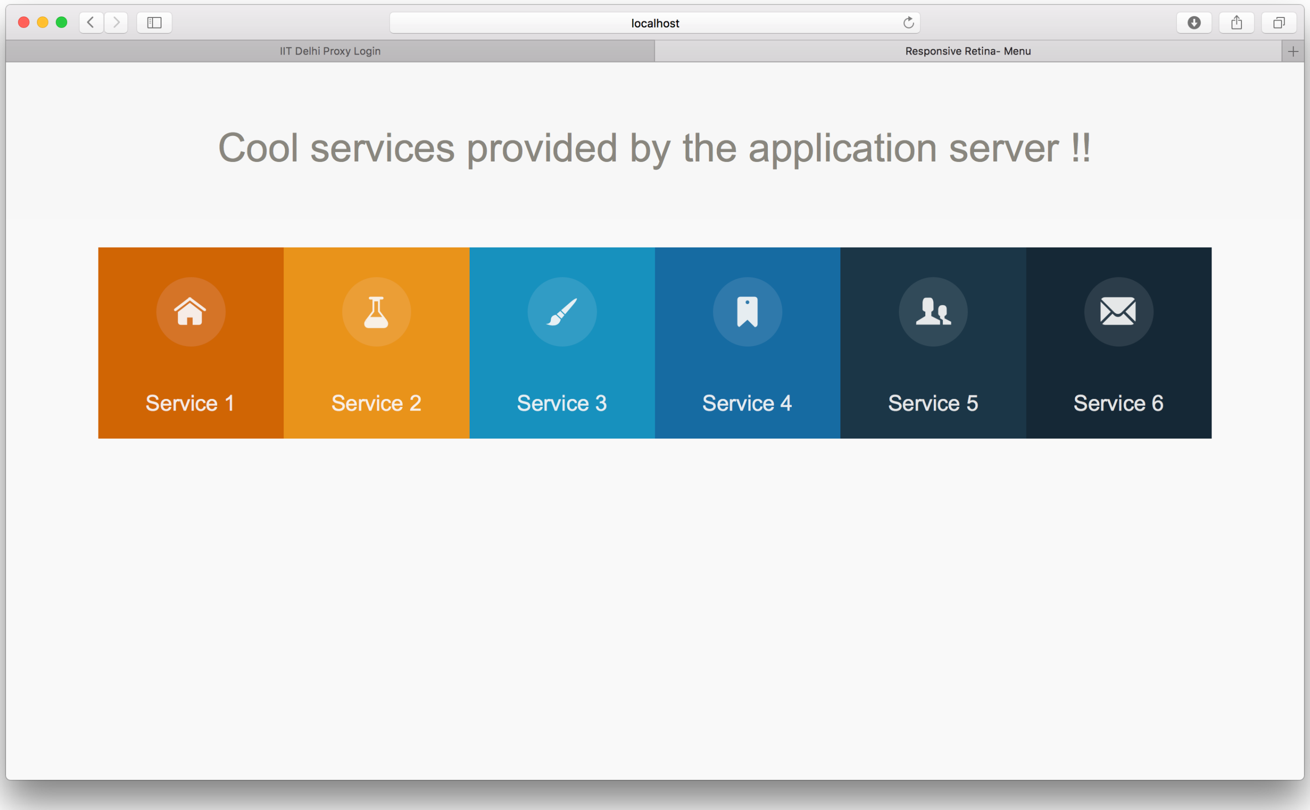

2. AS verifies user's access right in database, and creates ticket-granting ticket and session key. Results are encrypted using key derived from user's password.
once per user logon session
Kerberos
request ticket-granting ticket
ticket + session key
Authentication server
1. User logs on to workstation and requests service on host
request service-granting ticket
ticket + session key
Ticket-granting server (TGS)
once per type of service
4. TGS decrypts ticket and authenticator, verifies request, and then creates ticket for requested application server.
3. Workstation prompts user for password to decrypt incoming message, and then send ticket and authenticator that contains user's name, network address, and time to TGS.
request service
provide server authenticator
once per service session
5. Workstation sends ticket and authenticator to host.
Host/ application server
6. Host verifies that ticket and authenticator match, and then grants access to service. If mutual authentication is required, server returns an authenticator.

Figure 15.1 Overview of Kerberos

SCREEN SHOTS:





Cool services provided by the application server !!