Kerberos

• Trusted 3\textsuperscript{rd} Party Authentication Protocol
• Based on symmetric key cryptography (DES)
  – Based on Needham-Schroeder Authentication and Key Exchange Protocol
• Kerberos shares a different secret key with every network entity.
• Times must be synchronized between participants (NTP)
• MIT Project Athena Early 1980's
Kerberos - Cartoon

1 Request Ticket-Granting Ticket
2 Issue Ticket-Granting Ticket
3 Request Server Ticket
4 Issue Server Ticket
5 Request for service
Kerberos Protocol Definitions

- $s =$ server;  $c =$ client
- $a =$ client's network address
- $v =$ beginning and ending validity time for ticket
- $t =$ timestamp;  $K_X =$ X's secret key
- $K_{X,Y} =$ session key for X and Y
- $\{m\}K_X =$ m encrypted with X's secret key
- Ticket: $T_{c,s} =$ $s$, $\{c, a, v, K_{c,s}\}K_s$
- Authenticator: $A_{c,s} =$ $\{c, t, key\}K_{c,s}$
Kerberos Protocol

1. Client to Kerberos:
   c, tgs

2. Kerberos to Client:
   \{K_{c,tgs}\}K_c, \{T_{c,tgs}\}K_{tgs}

3. Client to TGS:
   \{A_{c,s}\}K_{c,tgs}, \{T_{c,tgs}\}K_{tgs}

4. TGS to client:
   \{K_{c,s}\}K_{c,tgs}, \{T_{c,s}\}K_s

5. Client to Server:
   \{A_{c,s}\}K_{c,s}, \{T_{c,s}\}K_s
Kerberos Protocol

1 Client to Kerberos:
   c, tgs

2 Kerberos to Client:
   \{K\_{c,tgs} \}\_{c}, \{tgs, \{c, a, v, K\_{c,tgs} \}\_{tgs}\}\_{tgs}

3 Client to TGS:
   \{c, t, key\}\_{c,tgs}, \{tgs, \{c, a, v, K\_{c,tgs} \}\_{tgs}\}\_{tgs}

4 TGS to client:
   \{K\_{c,s} \}\_{c,tgs}, \{s, \{c, a, v, K\_{c,s} \}\_{s}\}\_{s}

5 Client to Server:
   \{c, t', key'\}\_{c,s}, \{s, \{c, a, v, K\_{c,s} \}\_{s}\}\_{s}