SENG2250/6250 System and Network Security

School of Electrical Engineering and Computing

Semester 2, 2020

Lab 8: Distributed System Security

Objectives

1) Review Kerberos and OAuth2.0.
2) Learn Java socket programming.
3) Learn BigInteger class of Java for large number computation.

Part 1 Review Questions

1. What entities constitute a full-service Kerberos environment?

   Authentication server, ticket-granting server, service server, client.

2. In the context of Kerberos, what is a realm?

   A **realm** is a Kerberos server, set of clients and a set of application servers, such that:

   - The Kerberos server has the user ID's and hashed passwords of all participating users. All users are registered with the Kerberos server.
   - The Kerberos server shares a secret key with each server. They are "mutually" registered with other Kerberos servers.

3. Describe the message flow of Kerberos protocol version 4.

   1. C → AS: IDC, IDtgs, TS1
   2. AS → C: EKc[Kc,tgs, IDtgs, TS2, Lifetime2, Tickettgs]
      Tickettgs = EKtgs[Kc,tgs, IDC, ADC, IDtgs, TS2, Lifetime2]
   3. C → TGS: IDV, Tickettgs, AuthenticatorC
      AuthenticatorC = EKc,tgs[IDC, ADC, TS3]
   4. TGS → C: EKc,tgs[KC,V , IDV, TS4, TicketV]
      TicketV = EKv[Kc,v, IDC, ADC, IDV, TS4, Lifetime4]
   5. C → V: TicketV, AuthenticatorC
      TicketV = EKv[Kc,v, IDC, ADC, IDV, TS4, Lifetime4]
      AuthenticatorC = EKc,v[IDC, ADC, TS5]
   6. V → C: EKc,v[TS5 + 1]

4. What are the principal differences between version 4 and version 5 Kerberos?

    - Encryption: V4 uses DES only. V5 allows any encryption method.
    - Restricted ticket lifetime: V4 uses an 8-bit lifetime, for a maximum of about 21 hours. V5 allows the specification of start and end times.
    - Authentication forwarding: V4 does not allow credentials issued to one client to be forwarded to another host. Consider the following example of when this might be desirable: A client issues a request to a print server that then accesses the client's file from a file server, using the client's credentials. V5 allows such forwarding.
    - Offline double encryption of the tickets in steps two and four. This is unnecessary and inefficient. V5 removes the double encryptions.

5. What are the two tickets generated in (intra-realm) Kerberos protocol version 5? How could they be different in usage? Can we reuse these tickets?

    - Ticket-granting server ticket and service server ticket
    - Ticket-granting server ticket: is used for client authentication to the ticket-granting server.
    - Service server ticket: is used for client authentication to the service server.
    - It is possible to reuse the ticket, while there is a risk about the replay attacks.

6. What are the principle differences between the intra-realm Kerberos and inter-realm Kerberos protocols?

    In inter-realm Kerberos, a client has to communicate with the foreign Kerberos realm ticket-granting server to obtain the service ticket. It is different from the intra-realm scenario, because the home-realm ticket-granting server will give the client a ticket for foreign ticket-granting server authentication. The home-realm ticket-granting server cannot create a ticket for service server access.