Anon-Pass

Practical Anonymous Subscriptions

Introduction

- Anon-Pass is a protocol and a system for subscription services.
- It allows users to authenticate anonymously while preventing mass sharing of credentials.
- Service providers will not be able to correlate user's actions but are guaranteed that each account is in use at most once at given time.

Motivation

- It’s difficult to create systems that protect user privacy and simultaneously control admission.
- If users are required to log in to an account, foregoing anonymity, a service can enforce that no user is logged in twice simultaneously.
- A subscription system using a single shared identity for all users prevents user identification, but users could share the secret with nonsubscribers.
- The current cryptographic protocols for providing anonymous credential services require too much computation.

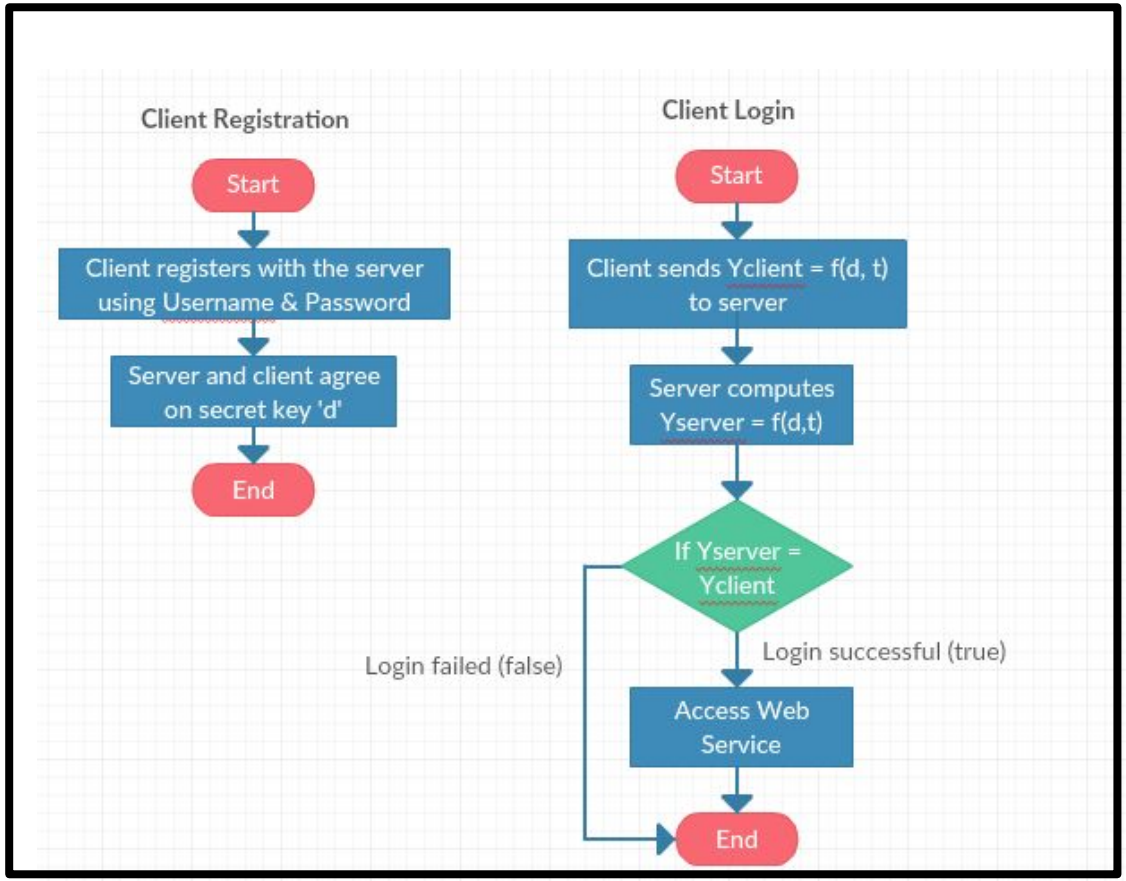
Problem Statement:

- To develop a Proof of Concept Model for Anon Pass Authentication System to preserve users Anonymity and also provide Admission Control for any Web Service.

Objectives

- To compare and contrast the three models of authentication.
- To perform a feasibility study on the advantages of using Anon-Pass Authentication over the other two methods.
- Develop the three authentication models.
- Analyse the performance of the three models.

Methodology of Basic Client Server Authentication



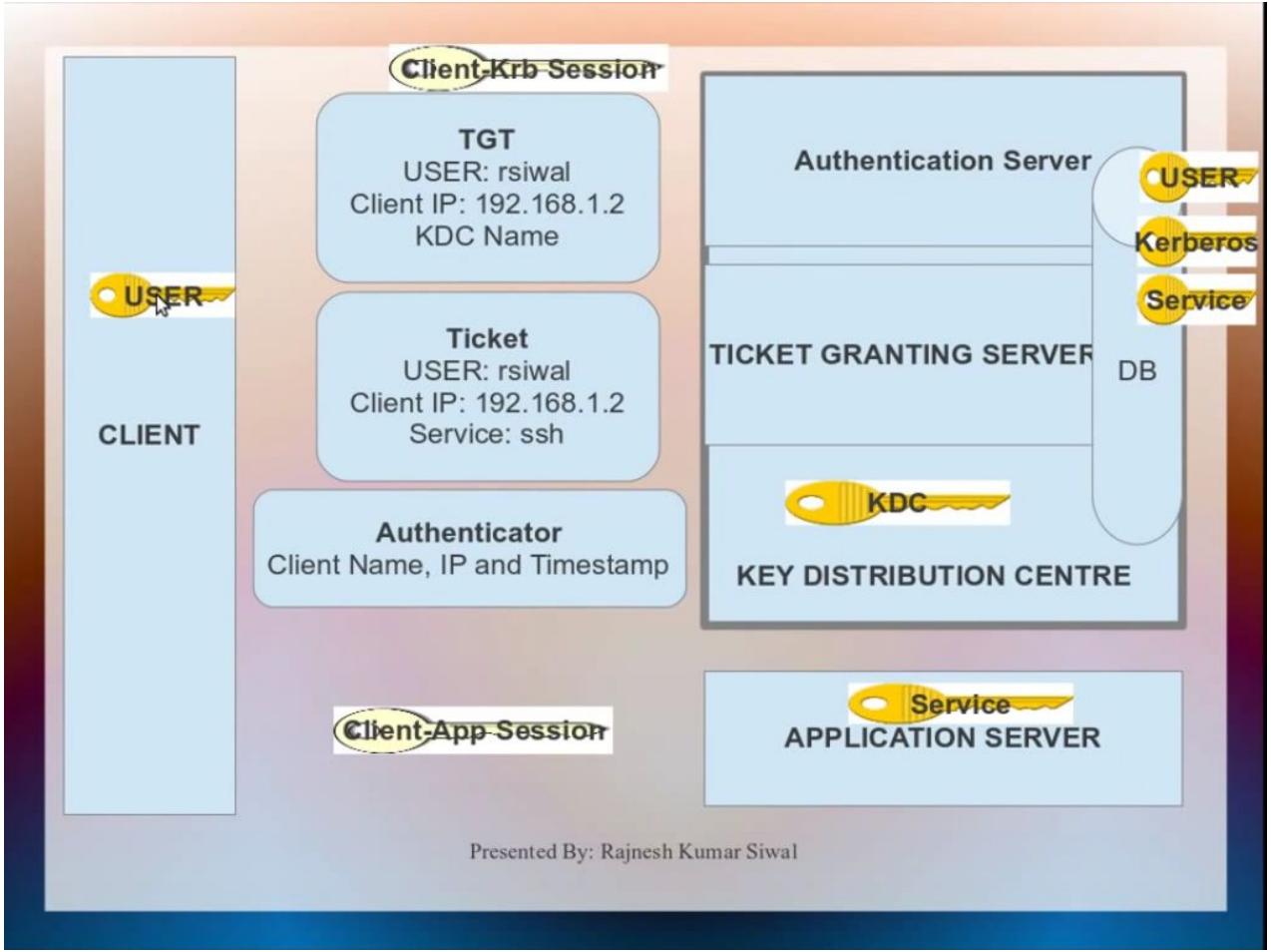
Disadvantages

- It is not flexible.
- Multiple logins are possible with the same credential.
- Computationally expensive cryptographic functions hinder the user experience , because the authentication and the web service is integrated in a single server.

Methodology of Kerberos

- **Step 1**: When the user logins to his or her machine. The username, is sent to KDC server for login, and the KDC server will provide TGT in return
- **Step 2**: Kdc server searches the principal name in the database, on finding the principal, a TGT is generated by the KDC, which will be encrypted by the users key, and send back to the user.
- **Step 3:** When the user gets the TGT, the user decrypts the TGT with the help of his/her private key. An important fact to note here is that, the client machine stores its key on its own machine only and this is never transmitted over wire.
- **Step 4:** The TGT recieved by the client from the KDC server will be stored in the cache for use for the session duration. There will always be an expiration time set on the TGT offered by the KDC server, so that an expired TGT can never be used by an attacker.
- **Step 5:** Now the client has got TGT in hand. If suppose the client needs to communicate with some service on that network, the client will ask the KDC server, for a ticket for that specific service with the help of TGT.

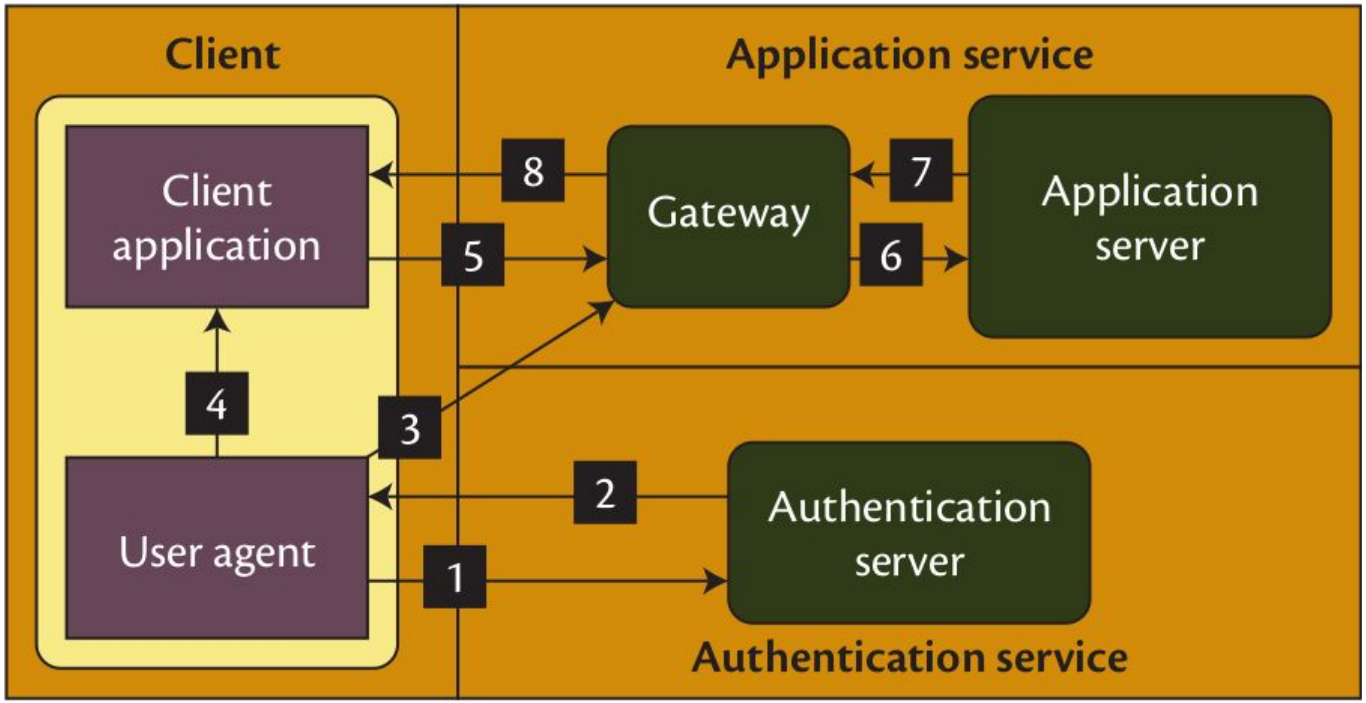
Methodology of Kerberos



Disadvantages of Kerberos

- Single Point of Failure: It requires continuous availability of the central server (KDC) . When the Kerberos server is down, new users can’t log in.
- Kerberos does not provide complete anonymity but it only provide pseudo anonymity. The Web Service has the ability to keep track and link an unknown users activity from time to time.

Methodology Of Anon Pass



Epochs

- Time is divided into equal-length intervals or epochs, agreed on by both clients and servers.
- The epochs are fed as input to PseudoRandom Function(PRF) which allows the users to change the login credentials for each epoch.
- Each client can create only one unique login credential per epoch which prevents multiple simultaneous logins with the same credentials.
- Service providers prefer long epochs to reduce the server load and users prefer short epochs to improve anonymity.

Implementation

- Client - Web Browser (HTML, CSS, JavaScript)
- Server - Python Script
- Communication between client and web server - PyWebSocket
- Three components of the Anon-Pass module
  - Registration, Login, and Re-Up
- Registration
  - Client sends username and password, server sends key ‘d’

Implementation continued...

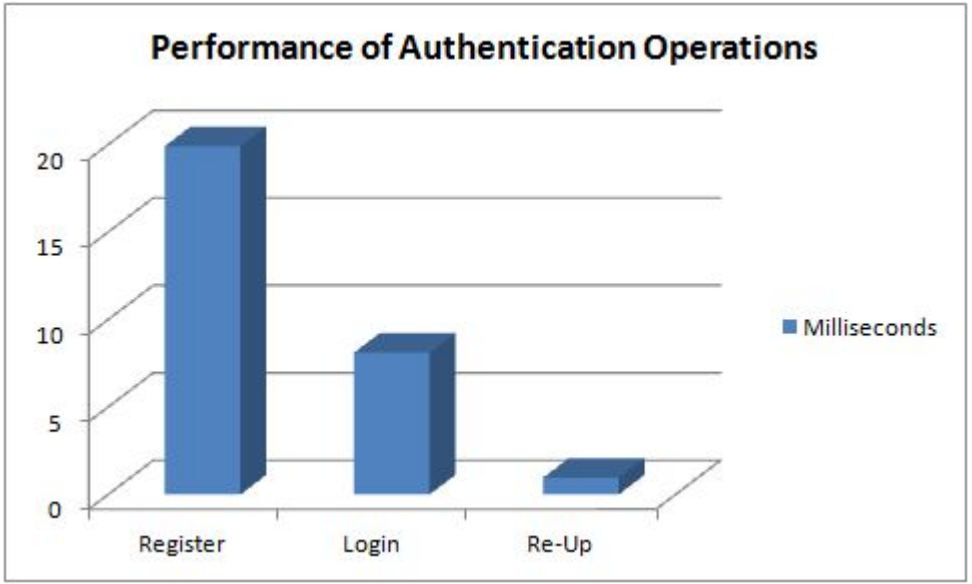
- Login
  - Server sends epoch number (t), client computes and sends Yclient = f(d,t)
  - The server generates its own list of Yserver values, and checks for the presence of Yclient in them
  - If present, the client is legit
  - If the client is legit, the server sends a token to allow the client to use the web service
- Re-up
  - Already logged in client send their Yclient values to the server. If their connection states are active, their Yclient values are retained. The rest are deleted.

Advantages of Anon Pass

- Provides unlinkability between user's actions in one or more sessions.
- Prevents abuse of service through sharing of credentials.
- The web service never communicates with the key distribution centre thereby anonymising the client's activity.

Results

Relationship between number of cores, models and maximum no. of requests made by the login system



No. of milliseconds taken for each protocol’s independent operation

Conclusion

- Basic authentication models suffers from a wide range of drawbacks.
  - High cryptographic computational cost, low flexibilty and the possibility of multiple logins.
- The Kerberos model suffers from a few drawbacks as well
  - Increased dependency on the Key Distribution Centre (KDC) for all activities pertaining to its operation
  - Issue of pseudo-anonymity.
- The Anon-Pass Authentication Model takes care of admission control and anonymity.

Future Work

- Anon-Pass System developed as a Proof of Concept Model.
- Application can be scaled to realise it in a full fledged commercial subscription system

References

[1] Michael Z. Lee, Alan M. Dunn,Jonathan Katz, Brent Waters, Emmett Witchel,"Anon-Pass: Practical Anonymous Subscriptions",IEEE S&P Symposium (2014), 20-27.
[2]Jan Camenisch, Susan Hohenberger, Markulf Kohlweiss, Anna Lysyanskaya, ,Mira Meyerovich," How to win the clone wars: Efficient periodic n-times anonymous authentication", ACM Conference on Computer and Communications Security(2006), 201–210.
[3] B. Clifford Neuman,Theodore Ts'o,"Kerberos: An Authentication Service for Computer Networks",IEEE Communications Magazine(1994),33-38.

Thank You

By
13IT104 Aditya Sriram
13IT107 Ashish K Singh
13IT135 Rohan R Nair
13IT251 Ohileshwar Itagi