Lecture Kerberos

Riccardo Torre

28 novembre 2025

Cos'è Servizio di autenticazione che fornisce un server di autenticazione centralizzato la cui funzione è di autenticare gli utenti ai server e i server agli utenti. Anche i server sono autenticati tra di loro.

Nota Kerberos fa uso solo ed esclusivamente di crittografia simmetrica!!!

Requisiti Kerberos Sicuro, trasparente, scalabile, affidabile.

Attori

1. **AS = authentication server:** conosce gli hash delle password di tutti gli utenti e li memorizza in un database centralizzato e crea ogni volta una chiave simmetrica con il client sfruttando l'hash della password come seme da passare a funzioni pseudo random; condivide un'unica chiave con tutti i server;
2. **TGS = ticket garanting server:**;

Ticket

- Ticket per entrare nel gioco che hanno una validità $Time_1$ ore $\rightarrow$ crittografia più forte;
- Ticket per utilizzare un servizio che hanno una validità $Time_2$ minuti $\rightarrow$ crittografia leggera;

$$Time_1 > Time_2$$

Man mano si usano ticket che durano sempre di meno.

Authenticator Chi sta operando e chi si dichiara sono la stessa persona.