Computer security

Technology, Information Technology

Computer Security Kerberos Computer Network Authentication Protocol

Kerberos serves as a network authentication protocol that allows for mutual identification, in which case the computer server and the user identify one another in the course of operation. The authentication situation involves three different parties; the user, the resources sourced for and the Key Distribution Centre (KDC) (Nagamalai, Renault and Dhanuskodi 496). Kerberos uses the KDC for authentication. The user logs in, and the principal sent to KDC server for login. The KDC server, in return, provides Ticket-Granting Tickets (TGT). The KDC server searches the principal name in the database and generates a TGT encrypted by the key generated and retrieved by the user. After the user gets the TGT, he or she decrypts the TGT using the KINIT (Kizza 214). The user's computer usually stores its key automatically but does not transmit it over the wire. The cache stores the TGT received from the KDC by the user for use during the session duration. However, the TGT has expiry duration set on it by the KDC after which the user cannot use it. With the help of TGT, the user can request KDC for a ticket to communicate with certain services within that network (Kizza 214). Kerberos are best applicable in management of highly confidential information within companies and institutions, where only one user can access information using a single entry key. With this authentication protocol, there is relatively reduced password piracy and database stealing. The authentication protocol enables easy implementation on embedded devices due to its one-way channel of authentication. Furthermore, there is mutual authentication of both the client and the server bringing about simplicity in inter-domain trust management (Dong and Chen 193).

Storage of the infrastructure login credentials in one central server renders the system vulnerable to data loss and contamination if an attacker found access to the location. Poor password creation of a user can make an attacker guess and find the password details right (Dong and Chen 193). Although Kerberos serves to block unencrypted users from using the internet services, if accessed by malicious users, the whole system may be at risk.

Works CitedTop of Form

Bottom of Form

Top of Form

Top of Form

Bottom of Form

Bottom of Form

Dong, Ling and Kefei, Chen. Cryptographic Protocol: Security Analysis Based on Trusted Freshness. Berlin: Springer, 2012. Print.

Kizza, Joseph. Guide to Computer Network Security. London: Springer, 2013. Print.

Nagamalai, Dhinaharan., Eric, Renault and Murugan, Dhanuskodi. Trends in Computer Science, Engineering and Information Technology: First International Conference on Computer Science, Engineering and Information Technology, Ccseit 2011, Tirunelveli, Tamil Nadu, India, September 23-25, 2011, Proceedings. Heidelberg: Springer, 2011. Print.