Kerberos is a network authentication protocol designed to provide strong authentication for client/server applications by using secret-key cryptography. It is a trusted third-party service that provides mutual authentication — both the user and the service verify each other's identity. Kerberos protocol is named after the three-headed dog from Greek mythology that guards the gates of the Underworld, symbolizing the protocol's role in protecting network security.

Here's how Kerberos works in a typical scenario:

1. **Authentication**: When a user attempts to access a service on the network, Kerberos authenticates the user's identity. The user submits a request for a "ticket" to the Kerberos authentication server (AS).
2. **Ticket Granting**: If the user's credentials are valid, the AS issues a Ticket Granting Ticket (TGT), which is encrypted and can only be decrypted by the Ticket Granting Server (TGS).
3. **Service Request**: When the user wants to access a network service, they request a service ticket from the TGS using the TGT.
4. **Service Access**: The TGS validates the TGT, generates a service ticket, and sends it to the user. The user then presents this service ticket to the network service they wish to access.
5. **Session**: The service decrypts the service ticket and establishes a secure communication session with the user.

Kerberos relies on symmetric key cryptography and requires a continuous time synchronization between all machines on the network because the tickets are time-stamped to prevent replay attacks.

**Single Sign-On (SSO)**, on the other hand, is a user authentication process that allows a user to access multiple applications with one set of login credentials. SSO is beneficial in a corporate environment where employees are required to access multiple applications and services; they can sign in once and gain access to all the necessary resources without being prompted to log in again at each of them.

Kerberos can be used to implement SSO within a network. Once the user is initially authenticated by Kerberos and receives their TGT, they can use that TGT to obtain service tickets for a variety of services within the network without needing to re-enter credentials. This creates a seamless user experience and is a practical example of SSO in action.

SSO reduces password fatigue for users, decreases the time spent re-entering passwords for the same identity, reduces IT costs due to lower number of IT help desk calls about passwords, and minimizes phishing, thus improving security. However, SSO can also pose a risk: if the primary authentication is compromised, it potentially gives an attacker access to all the user's accessible services.