System Administration

Authentication Across Network

Client

Internet

Server

user name
password

Problems?
System Administration

Secure Socket Layer

SSL

Client → server communication

1. Client connects
2. Server sends certificate
3. Client encrypts message using public key, sends to server
4. Server decrypts message using private key

Proven that with sufficient size of public/private keys, known computer power can not decrypt without private key.
- SSL: TCP socket is fully encrypted
- StartTLS: TCP socket, then client/server negotiate start of encryption.
- Clear: No encryption