Transport Layer Security (TLS)

TLS is the way that https and other secure ways of communicating with a remote server works. It is used to prove that the server you are connecting to is actually the one you expect. It also sets up an encrypted connection, so that the requests you send and the answer you receive are private between you and the remote server.

TLS is used to secure various Internet services such as web sites, e-mail, instant messaging and voice over IP (internet phone calls). It generally relies on public Certificates of Authority (CA's) which are standard in most operating systems.

TLS can also be used in an internal network (LAN) by creating a private Certifcate of Authority (CA) and manually adding this to internal machines. This allows for secure communications within your LAN, where public CA's are not available.

mTLS

mTLS is an extension of TLS to validate the client in addition to the server, allow the sysadmin to limit access to a service to validated users or programs. Read more about how this process works, and how to configure it.

See a more detailed explanation at Wikipedia

From:
https://kb.unixservertech.com/ - **Unix Server Tech Knowledge Base**

Permanent link:
https://kb.unixservertech.com/software/tls/start

Last update: **2025/07/23 20:32**