Mutual authentication

Mutual authentication or **two-way authentication** refers to two parties authenticating each other at the same time, being a default mode of authentication in some protocols (IKE, SSH) and optional in others (TLS).

By default the TLS protocol only proves the identity of the server to the client using X.509 certificate and the authentication of the client to the server is left to the application layer. TLS also offers client-to-server authentication using client-side X.509 authentication.[1] As it requires provisioning of the certificates to the clients and involves less user-friendly experience, it's rarely used in end-user applications.

Mutual TLS authentication (**mTLS**) is much more widespread in business-to-business (B2B) applications, where a limited number of programmatic and homogeneous clients are connecting to specific web services, the operational burden is limited, and security requirements are usually much higher as compared to consumer environments.

> Better institution-to-customer authentication would prevent attackers from successfully impersonating financial institutions to steal customers' account credentials; and better customer-to-institution authentication would prevent attackers from successfully impersonating customers to financial institutions in order to perpetrate fraud
>
> — Financial Services Technology Consortium, 2005

Most Mutual authentication is machine-to-machine, leaving it up to chance whether or not users will notice (or care) when the remote authentication fails (e.g. a red address bar browser padlock, or a wrong domain name). Non-technical mutual-authentication also exists to mitigate this problem, requiring the user to complete a challenge, effectively forcing them to notice, and blocking them from authenticating with a false endpoint.

Mutual authentication is of two types:

1. Certificate based
2. User name-password based

See also

- Computer security
- Digital signature
- Mobile signature