

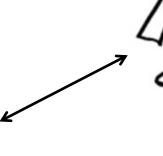
You're Web Browser

Personality A i.e. Locally Controlled Software

TLS + fig1 = end-to-end encryption & authentication

Personality B i.e. Remotely Controlled Software

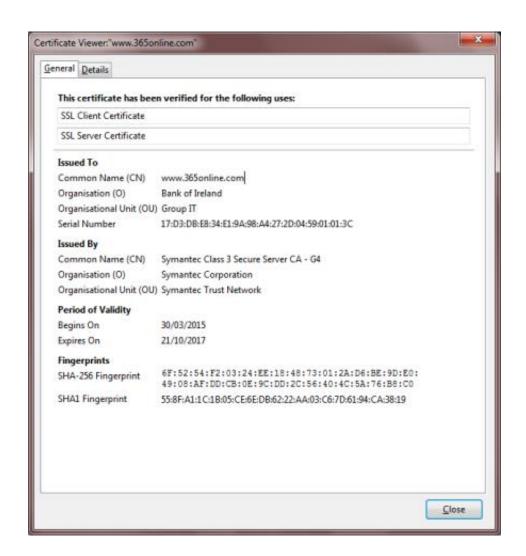
Phishing attack i.e. Bob replaced by Mallory due to failure to authenticate Bob. Fig1 forces authentication of Bob while preventing that process from being counterfeited.





Mallory

To solve phishing attacks we just need to help Alice to distinguish between personality A and personality B. We do this the same way cryptographers have been doing it for thousands of years i.e. we get personality A to authenticate itself by presenting a previously shared secret.





Current, hidden, identity information for user to authenticate and new window showing the same information from the TLS certificate i.e. it's TLS + authentication of which browser personality is 'in play'.