\subsection{SSL Vulnerabilities}

PKI infrastructure heavily relies on the security of the SSL Application Layer protocol and handshaking used to trade public and session keys.

Proposal to authenticate the user to avoid MITM attacks

SSL security is usually one way, server to user. Herzberg et al. propose a system, TPL, in which a certificate authority authenticates the user. \cite{herzberg2000access}

A Scheme to improve security of SSL - \cite{huawei2009scheme}

Proposes a new scheme (modify hand-shake protocol) which remedies the security defects of SSL as well as add valid SSL session key.

Certified lies: Detecting and defeating government interception attacks against ssl (short paper) - \cite{soghoian2012certified}