Goal of the System

The goal of SSL splitting is to reduce the bandwidth load on a server without losing the integrity of the data sent to a client. Data secrecy is explicitly not a goal of SSL splitting.

Trust Model

There are three entities in the SSL splitting protocol, the client, the server, and the proxy. The client trusts the server to provide a signature for the correct data. No other trust relationships exist.

Who is the adversary?

The adversary is a user on the network or a rogue proxy server.

What are the adversary's powers?

Both types of adversaries can perform man-in-the-middle attacks. In addition, they can can send their own legitimate requests to the server. They can also be thought to have access to the past and present server database.[1]

What constitutes a break of the system?

A break of the system occurs when a client accepts data as valid that is different than that endorsed by the server.

[1] In addition to the client/server request process, through channels available to proxies, adversaries can retrieve data from another proxy or directly from the server.