# Abstract

This thesis describes the implementation of Trusted Computing in end-to-end application security. It focuses on the services that are provided by application layer protocols in end-to-end communication. There are many security issues related to application layer protocols and some of these are explored. Application layer firewalls are often used to protect against these security issues. Unfortunately they are application specific, which means that only recognised protocols can be examined. It is practically impossible to distinguish between all possible application layer protocols. Therefore an abstraction to application layer protocols is proposed by providing a classification that tries to capture a large subset of the full spectrum of protocols. The security issues involved are discussed and addressed by Trusted Computing. A more thorough investigation is performed by examining the architecture of some distributed application components. Spam and secure message store in SMTP are researched and discussed in the context of Trusted Computing. Access control in FTP is enhanced to enable policy enforcement of an object on both the server and client platform. Furthermore, some ideas are proposed to enhance the privacy and security of web cookies. The research offers a new perspective on how Trusted Computing can improve end-to-end application security.