Abstract

This thesis investigates the protection landscape surrounding online banking. First, electronic banking is analysed for vulnerabilities and a survey of current attacks is carried out. This is represented graphically as an attack tree describing the different ways in which online transactions can be attacked.

The discussion then moves on to various defences which have been developed, categorizing them and analyzing how successful they are at protecting against the attacks given in the first chapter. This covers everything from TLS encryption through phishing site detection to two-factor authentication.

Having declared all current schemes for protecting online banking lacking in some way, the key aspects of the problem are identified. This is followed by a proposal for a more robust defence system which uses a small security device to create a trusted path to the customer, rather than depend upon trusting the customer’s computer. The protocol for this system is described along with all the other restrictions required for actual use. This is followed by a description of a demonstration implementation of the system.

Extensions to the system are then proposed, designed to afford extra protection for the consumer and also to support other types of device. There is then a discussion of ways of managing keys in a heterogeneous system, rather than one managed by a single entity.

The conclusion discusses the weaknesses of the proposed scheme and evaluates how successful it is likely to be in practice and what barriers there may be to adoption in the banking system.