

AN ANALYSIS OF SET PROTOCOL USING STRAND SPACE FORMAL TECHNIQUE

SHRADDHA SONI

Abstract

This paper presents an analysis of SET (Secure Electronic Transaction) popularly known for secure online payment using strand space model. The strand space model is one of the most rigorous formal methods used for analyzing cryptographic protocols. The analysis or the correctness proof of a protocol involves many properties like authentication, secrecy, non-repudiation etc. As per Lowe, there are different levels of authentication which can be proved for the two parties in a protocol run. This paper deals with the level of authentication achieved by the SET protocol.

Keywords: SET, Authentication, authentication test, strand space.