Scopus

Documents

Muhammad, S.

Applying authentication tests to discover Man-In-The-Middle attack in security protocols
(2013) *8th International Conference on Digital Information Management, ICDIM 2013*, art. no. 6693967, pp. 35-40. Cited 2 times.

Abstract
Authentication protocols ensure that participants in a distributed environment verify their identities before sending sensitive information to each other. If an authentication protocol has a design flaw, it may fail to reveal the true identities of distributed participants. To verify that an authentication protocol achieves its objectives, we have developed Authentication Tests based on Distributed Temporal Protocol Logic (DTPL). In this paper, we propose a generic strategy to analyze authentication protocols based on these Authentication Tests. We demonstrate the ease with which our proposed strategy can be used by applying these tests on famous Needham-Schroeder Public Key (NSPK) authentication protocol. We also demonstrate how the inability to prove a security property can lead us to identifying Man-In-The-Middle attack on such protocols. © 2013 IEEE.

2-s2.0-84893555327
Document Type: Conference Paper
Publication Stage: Final
Source: Scopus