Yuncheng Wang, Sep 13 2012 paper summary sheet

Paper title and authors; where appeared.

Breaking and Fixing the Needham-Schroeder Public-Key Protocol using FDR, Gavin Lowe, TACAS, 1996.

What is the main problem this paper attacks?

Lowe focuses on how to prove whether the Needham-Schroeder Public-Key Protocol is correct by using FDR, a protocol checking tool. He also manages to adapt the protocol and prove that if the Needham-Schroeder Public-Key is correct in a small system, then it is correct in an arbitrary size system.

What solution does the paper propose?

The paper proposes the detailed description of how to interpret the NS Public-Key Protocol in the FDR tool for CSP thus can find the flow of the protocol and adapt it manually. It also proposes a logic method to prove that if the NS is correct in a small system, then it is correct is correct in a lager one.

What central idea did the author use to solve it?

The intruder can do everything we could meet in the real world; we can prove that if the larger system is attacked then the small system must have flow, which is simpler way to solve the second part problem.

What is a weakness or limitation of the paper?

The author says that he intend to analyze more protocols and produce more lemmas and theorems in the logic method. He also hopes to identify the properties of protocols to directly prove the protocol is correct.

Why is the paper important?

This paper proposes a logic method to prove that if NS Public Key Protocol is correct in a small system then it is practical in a lager system. This method seems can be applied in a general protocol and implies a way to prove whether a protocol is correct.