

OFMC : On-the-fly Model Checker or Open-Source Fixed-Point Model Checker

A symbolic model checker for analysis of Security Protocols

A presentation by Julien Caron, Benoit Dequidt, Antoine Lefebvre and Jérémie Stordeur

We introduce the Open-Source Fixed Point Model Checker OFMC for symbolic security protocol analysis, previously known as the On-the-fly Model Checker explained in the articles [1] and [2].

We then discuss about symbolic techniques and optimizations for modelling a lazy Dolev-Yao intruder. The Dolev-Yao threat model represents that can overhear, intercept and synthesise any message and is only limited by the constraints of the cryptographic methods used. The lazy intruder is an optimization technique that significantly reduces the attack search tree.

We will present the two syntaxes used by OFMC, first the Intermediate format IF which is the one used in AVISPA and secondly Alice And Bob AnB syntax, which is a new high-level and simpler language brought in the new OFMC version.

Moreover we will see the improvements of this new version: use of over-approximation, definitions of algebraic relations such as associativity, commutativity and also specifications on channels' secrecy level: authenticity, confidentiality and integrity point of view.

To conclude, we will see some experimental results that David Basin, Sebastian Mödersheim and Luca Viganò obtained on 38 protocols from the Clark/Jacob library. We will study the new attack found on the H.530 protocol.

References:

[1] David Basin, Sebastian Moedersheim, and Luca Viganò. *OFMC: A symbolic model checker for security protocols*. In *International Journal of Information Security*, 4 (3), pages 181-208, 2005.

[2] Sebastian Moedersheim and Luca Viganò. *The Open-source Fixed-point Model Checker for Symbolic Analysis of Security Protocols*. *Fosad 2007-2008-2009, LNCS 5705*, 166-194. Springer-Verlag, 2009.