Keeping Fairness Alive

Torabi Dashti, M.

2008

document version
Publisher's PDF, also known as Version of record

Keeping Fairness Alive

Design and formal verification of optimistic fair exchange protocols

M. Torabi Dashti

This thesis can be divided into two parts on *designing* and *verifying* optimistic fair exchange protocols.

In the first part, we propose a novel fair certified email protocol. A certified email protocol enables Alice to send an email to Bob in exchange for a receipt. The receipt is a proof that shows Bob has received the email. A fair certified email protocol guarantees fairness in this exchange: Bob receives the email if, and only if, Alice receives the receipt. Such exchanges are in general impossible, unless a trusted party is (at least marginally) involved in the protocol. The novelty in our protocol pertains to using key chains to reduce the amount of the storage that the trusted party requires to maintain fairness.

In the second part, we develop an intruder model along with a carefully crafted fairness constraint to enable verifying liveness aspects of optimistic fair exchange protocols. This intruder model is equivalent to the standard Dolev-Yao intruder model, except that it is not allowed to indefinitely delay messages over the so-called resilient communication channels. Resilient channels are instrumental in most optimistic fair exchange protocols. As an empirical basis for the effectiveness of the proposed model, a fair payment protocol and a fair digital rights management scheme are formally analysed using this intruder.

Furthermore, we extend an existing partial order reduction algorithm for security protocols to the case of optimistic fair exchange protocols. A unique feature of these protocols is that their participants are usually provided with certain choice points in the course of each exchange, and such choice points require special treatments in the reduction algorithm. The scalability and effectiveness of the proposed reduction algorithm are shown in a few case studies.