Keeping Fairness Alive

Torabi Dashti, M.

2008

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

Samenvatting

Eerlijk duurt het langst
Ontwerp en formele verificatie van optimistische fair exchange protocollen

Dit proefschrift bestaat uit twee gedeeltes, namelijk het *ontwerp* en de *verificatie* van optimistische "fair exchange" protocollen.

Het eerste gedeelte draait om een nieuw gecertificeerd email-protocol, waarmee Alice een email naar Bob kan sturen, in ruil voor een ontvangstbewijs. Dit is een fair exchange protocol: Bob ontvangt de email dan en slechts dan als Alice het ontvangstbewijs krijgt. Een dergelijke uitwisseling is alleen mogelijk indien een vertrouwde derde partij bij het protocol betrokken is. De kracht van het protocol ligt in het gebruik van sleutel-ketens, waardoor deze derde partij minder opslagruimte nodig heeft om fairness te kunnen garanderen.

In het tweede gedeelte wordt een modellering van indringers, met een zorgvuldig ontworpen fairness beperking, ontwikkeld die het mogelijk maakt om liveness aspecten van optimistische fair exchange protocollen te verifiëren. Ons indringer-model is equivalent met het standaard Dolev-Yao indringer-model, behalve dat ieder bericht dat door een communicatiekanaal wordt verstuurd uiteindelijk zijn bestemming dient te bereiken. Dergelijke betrouwbare communicatiekanalen zijn cruciaal in de meeste optimistische fair exchange protocollen. Om op empirische wijze de effectiviteit van ons indringer-model aan te tonen, worden twee protocollen voor electronische betaling en voor digitale rechten formeel geanalyseerd op basis van dit model.

Verder wordt een bestaande "partiële ordening reductie" techniek uitgebreid, zodat deze techniek toepasbaar wordt op optimistische fair exchange protocollen. In deze protocollen hebben de deelnemers gedurende de uitwisseling gewoonlijk zekere keuzemomenten, die een speciale behandeling vereisen in de partiële ordening reductie techniek. De schaalbaarheid en effectiviteit van de techniek worden door middel van enkele case studies aangetoond.