Protocollen en compositie

Voordracht door: Pieter Rogaar
Datum: 19 maart 2008
Begeleider: Dennis Hofheinz

Een protocol is een manier voor een aantal partijen om een doel te bereiken door op een vooraf afgesproken manier te handelen en te communiceren. Deze partijen zijn bijvoorbeeld onderhandelaars die een contractonderhandeling willen voeren, een burger die digitaal zijn stem uit wil brengen bij een overheid of een systeembeheerder die op afstand zijn server wil kunnen besturen.

Natuurlijk is het doel vaak eenvoudig te bereiken als de legitieme partijen de enigen zijn die deelnemen aan het protocol. Om realistischer uitspraken te doen kiezen we er daarom voor een minder reine omgeving voor te stellen, waarin allerlei kwaadwillenden zich in kunnen laten met het verkeer dat op het netwerk plaatsvindt. Ze kunnen dan berichten afluisteren, veranderen, verwijderen of zelfs oude berichten herhalen of nieuwe zelf-geconstrueerde toevoegen. Deze 'tegenstanders' laten we allemaal samenwerken tegen het protocol om een zo sterk mogelijke notie van veiligheid te bereiken.

De doelen die heden ten dage gesteld worden, kunnen zeer complex van aard zijn. Van de protocollen die hiermee corresponderen, zijn daardoor ook lastig veiligheidseigenschappen te verifiëren. Het liefst willen we naar een modulaire opbouw van dergelijke protocollen, omdat bepaalde veiligheidseigenschappen van een module overeen kunnen komen met een ideale functionaliteit, waardoor deze module implementeren automatisch zorgt voor de gewenste eigenschappen van het totale protocol.

Vergelijk dit bijvoorbeeld met het doel van de contractonderhandeling: Een partij zal een beveiligde verbinding willen met de andere kant, voor er gegevens uitgewisseld worden. Helaas is dit niet het enige doel, en kunnen de verschillende wijzen waarop doelstellingen gerealiseerd worden, ervoor zorgen dat de communicatie niet bewijsbaar veilig is. Als we een modulaire aanpak kunnen kiezen, bouwen we een module 'beveiligde communicatie' en kunnen de ideale functionaliteit van beveiligde communicatie implementeren met behulp van de module 'beveiligde communicatie'.

De stelling die deze implementatie van modules beschrijft, heet de compositiestelling, en kort gezegd geeft deze een aantal voorwaarden waaraan een module moet voldoen voor deze een veilige realisatie van de ideale functionaliteit geeft. Wat de omgeving (de partijen en de tegenstanders) dan ook met het protocol doen, het geheel blijft de eigenschappen van de module implementeren. Deze stelling kan in verschillende niveaus van algemeenheid geformuleerd worden, waarbij het onderscheid vooral bestaat tussen *hoe veel* instanties van de module tegelijk geïmplementeerd mogen worden.

Verschillende onderzoekers hebben een raamwerk geschapen waarbinnen deze stelling bewezen kan worden. Canetti beschrijft vrij sterke eisen in zijn kader van 'Universal Composability'. Deze vrij sterke eisen van samenstelbaarheid geven een zeer algemene stelling, waarbij een willekeurig aantal instanties van de module geïmplementeerd kan worden. Maurer, Renner en Holenstein geven een zwakker kader (waarin dus meer protocollen beschreven kunnen worden), waarin de algemene stelling bewijsbaar onjuist is. Als dit kader, dat niet alleen zwakker maar ook anders van aard is, versterkt wordt, kan de algemenere stelling mogelijk wel beschreven en bewezen worden.