Geleitwort

Seit den siebziger Jahren des letzten Jahrhunderts wird intensiv auf dem Gebiet der kooperativ-intelligenten Systeme geforscht. Zunächst standen intelligente Lösungen für die Aufgabenverteilung an sogenannte "Problemlösungsknoten" im Vordergrund. Bahnbrechende Lösungen dieser Zeit sind in Stanford, am MIT und an der Carnegie Mellon University entstanden. Beispiele sind das Contract Net Protocol, die Blackboard-Architektur und das von Rosenschein entwickelte Konzept des autonomen Software-Agenten. Dieses eröffnete Mitte der achtziger Jahre Zugänge zu Themenbereichen, die im allgegenwärtigen Internet höchste Relevanz besitzen: Verhält sich ein Agent bei Übernahme einer Aufgabe tatsächlich so, wie er es angekündigt hat? Ist er kooperativ oder antagonistisch, konfliktfreudig oder risikoscheu? Lügt er gar, und muss man ihn – kann man ihn überhaupt – gegebenenfalls zu einem bestimmten Verhalten zwingen? Mit anderen Worten: Kann man sich denn überhaupt auf einen Software-Agenten verlassen?

Bis Ende der 90er Jahre war dies ein einseitiges Problem. Bis dahin genügte es, (Autonomie einschränkende) technische Vorkehrungen zu treffen, um das Agentenverhalten zuverlässig vorhersehbar zu machen. Dies änderte sich jedoch grundlegend mit der Programmiersprache Java. Nun konnten bis dahin fest mit ihrer Ausführungsplattform verbundene Agenten aufgrund eigener Entscheidung von einer Ausführungsplattform zur anderen migrieren. Damit stellte sich sofort die Frage des Schutzes vor "feindlich gesonnenen" Ausführungsplattformen: das Malicious-Host-Problem war geboren.

Wenn ein Agent eine virtuelle Geldbörse mit sich führt, um auf dem Weg durch ein Computernetzwerk Dienstleistungen Dritter einkaufen und selbst Leistungen gegen Geld erbringen zu können, müssen er selbst, aber auch das Gesamtsystem vor "Malicious Hosts" geschützt werden. Ein Kernproblem ist hier das Host getriebene Double Spending. Dabei bereichert sich ein Host durch Vervielfältigung des von einem Agenten mitgeführten elektronischen Geldes. Dieses Problem ist bis heute nicht gelöst.

Christian Anhalt adressiert diese Herausforderung mit einer Lösungsarchitektur, die konzeptionell auf der doppischen Rechnungslegungstheorie beruht. Die didaktisch höchst gelungene Aufbereitung des komplizierten Stoffs eröffnet die von ihm dann auch konsequent genutzte Chance, seinen konzeptionell originellen Ansatz sehr kompakt und in weitgehend redundanzfreier Form zu entwickeln. Als Ergebnis steht uns nun ein optimistischer Lösungsansatz zur Verfügung, der im Gegensatz zu bisherigen Vorschlägen grundsätzlich davon ausgeht, dass alle im Gesamtsystem zu beobachtenden Aktionen zulässig sind. Erst nachträglich wird auf Basis fortlaufend protokollierter

Kontenstände überprüft, ob Double-Spending-Situationen eingetreten sind und welche Akteure daran beteiligt waren sowie entschieden, wie darauf im Einzelfall zu reagieren ist.

Damit gestattet dieser von Christian Anhalt vollständig neu entwickelte Lösungsansatz den Einsatz funktionstüchtiger und gegenüber Double Spending sicherer münzbasierter Bezahlsysteme für mobile Agenten in offenen Systemen. Er enthält darüber hinaus das Potenzial, auch im Kontext anderer Angriffstypen sichere Lösungen hervorzubringen. Aus diesem Grund und angesichts der hohen praktischen Relevanz von Sicherheitsfragen im Intenet-basierten Geschäftsverkehr wünsche ich der vorliegenden Arbeit eine zahlreiche Leserschaft und eine weite Verbreitung.

Univ.-Prof. Dr. Stefan Kirn