Gerald Brose: Access Control Management in Distributed Object Systems

Dissertation am Fachbereich Mathematik und Informatik, Freie Universität Berlin

Disputation: 17. Oktober 2001

Gutachter: Prof. Dr. Klaus-Peter Löhr (FU Berlin),
Prof. Dr. Dieter Gollmann (Microsoft Research, Cambridge, UK)

Zusammenfassung:

Das Thema der Arbeit ist eine geeignete Unterstützung für die Spezifikation, die Installation und das Management von Zugriffsschutzpolitiken. Eine solche Unterstützung erhöht die Gesamtsicherheit eines verteilten Objektsystems, indem zum einen der flexible Ausdruck von Sicherheitsanforderungen erleichtert und zum anderen gleichzeitig eine grosse Zahl möglicher Fehlerquellen ausgeschlossen wird. Die Arbeit untersucht zunächst Anforderungen an handhabbaren Zugriffsschutz. Die Aufgabe des Zugriffsschutzmanagements wird analysiert und in Unteraufgaben gegliedert, die von verschiedenen, voneinander getrennten Managern wahrgenommen werden können, nämlich die Verwaltung von Principals und Zertifikaten, von Objekten und Domänen, sowie die Politikverwaltung selbst. Darüberhinaus wurden die Aufgaben der Politikinstallation und -entwicklung betrachtet. Aus der Analyse der Anforderungen an die Dokumentation, die Unterstützung der Kommunikation zwischen den Beteiligten und die benötigten Sprachkonzepte ergibt sich, dass ein integrierter Ansatz für die Entwicklung und das Management von Zugriffsschutzpolitiken am besten durch die Definition einer deklarativen Politiksprache unterstützt werden kann.

Der Beitrag dieser Arbeit besteht in einem neuen, sichtenbasierten Zugriffsschutzmodell und einer deklarative Politiksprache namens View Policy Language (VPL), das den genannten Anforderungen genügt. Die Abstraktionen dieser Sprache wurden speziell für die Unterstützung sowohl des Entwurfs wie der Installation und des Managements von Politiken entworfen. Die zentralen Sprachkonzepte von VPL sind Sichten als ein first-class Konzept für die typsichere Aggregation von Zugriffsrechten, Rollen als aufgabenorientierte Abstraktion von Aufrufern, sowie Schemata als Mittel zur Spezifikation automatisch ausgelöster, dynamischer Änderungen des Schutzzustandes.

Die praktische Relevanz dieser Konzepte wurde durch die Implementierung einer realistischen Fallstudie gezeigt. Das Beispiel zeigt die Verwendung von Rollen, Sichten, Schemata, negativen Rechten und bedingten Sichten im Kontext eines Systems zur Begutachtung eingereichter Konferenzbeiträge. Die technische Machbarkeit sichtenbasierten Zugriffsschutzes wurde durch die Implementierung der erforderlichen Sicherheitsinfrastruktur für CORBA nachgewiesen. Die Implementierung umfasst einen Interceptorbasierten Zugriffsschutzmechanismus, einen VPL-Übersetzer, Sichten- und Rollenrepositories sowie graphische Managementwerkzeuge.

Das Dokument ist als PDF-Datei erhältlich unter:
`http://www.diss.fu-berlin.de/2001/203/` sowie über die Homepage des Autors:
`http://www.inf.fu-berlin.de/~brose/`