C Zusammenfassung in deutscher Sprache

Das zentrale Thema dieser 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, möglicherweise getrennten Managern wahrgenommen werden, nämlich die Verwaltung von Principals und Zertifikaten, von Objekten und Domänen, sowie die Politikverwaltung selbst. Darüberhinaus wurden auch 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 nachgewiesen, die einen Interceptor–basierten Zugriffsschutzmechanismus, einen VPL–Übersetzer, Sichten– und Rollenrepositories sowie graphische Managementwerkzeuge umfaßt.