Schönbein, R., Bügel, U., & Leuchter, S. (2005). Semantic Web Technologien für Sicherheitsaufgaben. *Informatik 2005 – 35. Jahrestagung der Gesellschaft für Informatik, Symposium: Tag der außeruniversitären Forschung*. Bonn: 19.09.2005. http://www.safety-critical.de/doc/info2005TAF.pdf

# Semantic Web Technologien für Sicherheitsaufgaben

Rainer Schönbein, Ulrich Bügel & Sandro Leuchter

Fraunhofer Institut für Informations- und Datenverarbeitung IITB
Fraunhoferstr. 1
D-76131 Karlsruhe
{rainer.schoenbein, ulrich.buegel, sandro.leuchter}@iitb.fraunhofer.de

**Abstract:** In diesem Beitrag werden ontologie-basierte Technologien und ihr Einsatz in sicherheitsrelevanten Anwendungen vorgestellt. Ontologien werden verwendet, um heterogene Daten-, Informationsquellen und Dienste unterschiedlicher Behörden und Organisationen mit Sicherheitsaufgaben auf semantischer Ebene zu verknüpfen. Abhängig vom Einsatzszenario wird das so repräsentierte Wissen durch SW-Agenten genutzt oder durch Content-Management-Systeme zur Verfügung gestellt.

## 1 Anwendung

Öffentliche Sicherheit umfasst sowohl den Schutz vor zufällig oder fahrlässig entstehender Gefährdung (*Safety*) als auch vor absichtlich herbeigeführter Gefährdung (*Security*). Die Gewährleistung der öffentlichen Sicherheit ist eine hoheitliche Aufgabe. Sie wird in Deutschland von einer Vielzahl von Behörden und Organisationen wahrgenommen (BOS: Behörden und Organisationen mit Sicherheitsaufgaben). Die Zusammenarbeit zwischen BOS ist schwierig, denn es fehlen Schnittstellen für einen computergestützte Informations- und Dienstaustausch, teils auch in Ermangelung rechtlicher Grundlagen. Das organisatorische und technische Problem besteht in der Zusammenführung heterogener Datenquellen, in die von unterschiedlichen Stellen aktuelle Erkenntnisse eingespeist werden. Die Zusammenführung ist erforderlich, um ein aktuelles und umfassendes Lagebild zu erhalten, das für den spezifischen Informationsbedarf der anfragenden Stelle zurechtgeschnitten ist. Es geht dabei nicht nur um rohe Daten, die in der Regel nur von den jeweiligen Fachleuten interpretiert werden können, sondern insbesondere um daraus abgeleitete Erkenntnisse und Expertisen. Das Spektrum der Nutzer der realisierten und zukünftig denkbaren Anwendungen reicht von interessierten Privatpersonen über Behördenvertreter mit konkreten Aufgaben bis zu Angehörigen des Militärs. Der Informationsbedarf dient entweder der Bekämpfung eines eingetretenen Ereignisses (Katastrophen-Management) oder dem planvollen Umgang mit Risiken, um den Schadensfall zu verhindern bzw. seine Auswirkungen zu minimieren (Risiko-Management).

Am Fraunhofer IITB werden Anwendungen auf der Basis von *Semantic Web*-Technologien [BHL01] entwickelt, um heterogene Informationsquellen zu verknüpfen. Ziel ist eine transparente, rollenbasierte Vermittlung von Informationen. Die Datenquellen und Dienste, die dafür herangezogen werden, müssen auf syntaktischer Ebene interoperabel sein. Darüber hinaus müssen ihre Inhalte formal beschrieben werden, damit eine semantische Verknüpfung möglich wird. Die Nutzung der Informationsquellen geschieht entweder auf Initiative eines Benutzers oder asynchron.

## 2 Realisierungen

Das EU-Projekt ORCHESTRA (*Open Architecture and Spatial Data Infrastructure for Risk Management [O05]*) hat das Ziel, eine offene dienstorientierte Software-Architektur zu erstellen, die eine integrierte Betrachtung von raum-, zeit- und sachbezogenen Informationen mit einem ontologie-basierten Ansatz ermöglicht. Dadurch soll ein domänen- und grenzüberschreitendes *Multi-Risk Management* realisiert und erprobt werden. So können beispielsweise Daten über einen Waldbrand in einem grenznahen Gebiet als Eingabe zur Untersuchung des - aufgrund des massiven Eingriffs in die Vegetation nun erhöhten - Flutrisikos genutzt werden. Das Fraunhofer IITB ist in diesem Projekt für die Software-Architektur verantwortlich.

Das Fraunhofer IITB ist im Auftrag des Bundesamtes für Wehrtechnik und Beschaffung gemeinsam mit der Firma EADS an der Entwicklung des intelligenten Sensor-Verbundes Aufklärung (ISVA [SM+04]) beteiligt. Hier geht es um die agentenbasierte Suche nach Personen, Informationen und Dienstleistungen auf dem Themengebiet der Fernerkundung zur Aufklärung und Überwachung, insbesondere zur interaktiven Bildauswertung. Die verwendete Ontologie beschreibt daher Prozesse, Komponenten und Dienste der Bildauswertung sowie die in Bildern abgebildeten Objekte und deren Zusammenhänge und darauf aufbauend Konzepte und Relationen zur Fernerkundung.

Das Eigenforschungsprojekt ExperOnto [LSU05] zielt darauf ab, neue Wissensrepräsentationsformate zu erproben und den technologischen Ansatz auf das kompetenzgesteuerte Zusammenstellen von Projektteams zu übertragen. Hier werden Personen-, Kompetenz-, und Projektressourcen-Ontologien benutzt, um organisationsübergreifend nach Experten mit bestimmten Expertise-Profilen zu suchen und unter Berücksichtigung von freien Ressourcen Teams zusammengebracht.

## 3 Technologien

In den Anwendungen werden Ontologien verwendet, die den Gegenstandsbereich anhand seiner Konzepte, deren Relationen und zusätzlicher Regeln repräsentieren. Ontologien werden mit unterschiedlichen Beschreibungstechniken formalisiert (s. z.B. [SS05]). Es gibt eine Bandbreite von Formalismen von einfach handhabbaren Formaten bis hin zu mathematisch beschriebenen logischen Kalkülen. Gerade bei Ontologien im Sicherheitsbereich, wo es die Anforderung geben kann, große Gruppen von Individuen zu charakte-

risieren, ermöglicht die Verwendung von Beschreibungslogik eine deutliche Reduzierung des Modellierungsaufwandes.

Auch der Aufbau technischer Informationssysteme zur intelligenten Ablage eines Dokumentenbestandes stützt sich meistens auf eine Kategorisierung der zu speichernden Information in anwendungsspezifische Wissensbausteine mit zugehörigen Erfassungsmasken und Darstellungstemplates. Erfahrungen in verschiedenen Projekten belegen die Notwendigkeit, diese Wissensbausteine in einem semantischen Netzwerk miteinander zu verknüpfen, um sie so in einen Kontext einbetten zu können. Die in einigen der beschriebenen Projekte zum Einsatz kommenden Content-Management-Systeme bieten zur Unterstützung der Vernetzung ein automatisches Beziehungs-Management auf Basis von Ontologien an.

Der Einsatz von SW-Agenten ermöglicht hingegen eine regelgesteuerte Verknüpfung von verteilten Informationsquellen. Beim Planen von komplexen Informationszusammenstellungen können sie alternative Dienste und Quellen anhand inhaltlicher Vorgaben vergleichen und auch Kosten-/Nutzenmodelle berücksichtigen: Beispielsweise bringt eine höhere Auswertegenauigkeit einen erhöhten Zeitaufwand mit sich, der je nach Anwendung nicht vertretbar sein kann. Agenten können asynchron zu Nutzerinteraktionen das Auftreten von Ereignissen erkennen und pro-aktiv handeln.

## 4 Ausblick

Bei der Nutzung von heterogenen Informationsquellen ist Vertrauen in besonderem Maße relevant. Nutzer müssen sicher sein können, dass angebotene Informationen und ihre ontologische Beschreibung korrekt sind. Unter beschränkten Ressourcen sind jedoch weder vollständige Sicherheit noch vollständige Korrektheit erreichbar. Deshalb müssen Maße für Qualität und Vertrauen herangezogen werden, die im Kosten-/Nutzenmodell analog zu *quality of service* Infrastrukturen in Kommunikationsnetzen oder wie in *Recommender*-Netzwerken [RV97] verankert sein könnten.

Bei sicherheitsrelevanten Anwendungen ist die Authentifizierung von Nutzern und Informationsanbietern in ihren institutionellen Rollen entscheidend. Wenn die Zusammenarbeit von BOS in diesem Bereich durch neue Technologien ermöglicht wird, muss eine zentrale Authentifizierungsinstanz z.B. in Form einer PKI, die allen potentiellen Akteuren offen stehen muss, eingerichtet werden und entsprechende Zugriffsrechte für Organisationen, Nutzer und ihre Agenten definiert werden.

Die vorgestellte Technologie hat auch potentielle Anwendungen außerhalb des Sicherheitsbereiches: Die Service orientierte Architektur (SOA) bietet inzwischen eine technologische Plattform für verteilte Geschäftsanwendungen, die aus interoperablen Komponenten entlang der Wertschöpfungskette eines Unternehmens zusammengesetzt werden. Für Anwendungen beim *Service Engineering* fehlt aber bislang eine Unterstützung der Dienstbeschreibung auf der semantischen Ebene. Deshalb werden Werkzeuge und Infrastrukturen für eine automatische Konfiguration von virtuellen Unternehmen bislang nicht angeboten. Die vorgestellte Technologie bietet hier einen Lösungsansatz. Im Ver-

gleich zu abgegrenzten Sicherheitsdomänen erfordert jedoch die allgemeine Wirtschaft vergleichsweise umfangreiche Ontologien.

## Literaturverzeichnis


[BHL01] Berners-Lee, T.; Hendler, J.; Lassila, O.: The Semantic Web. *Scientific American*, May 2001.

[LSU05] Leuchter, S.; Schönbein, R., Urbas, L.: Skalenfreie Netzwerke und Benutzermodellierung. *Informatik 2005;* in diesem Band.

[O05] ORCHESTRA Executive Board: *Towards an open disaster risk management service architecture for INSPIRE and GMES*. Online-Dokument: http://www.eu-orchestra.org/docs/20050223_White%20Paper_v9.pdf (letzter Zugriff: 20.05.05), 2005.

[RV97] Resnick, P.; Varian, H.: Recommender Systems. *Communications of the ACM*, 40, S. (3) 56-58; 1997.

[SM+04] Schönbein, R.; Mühlenberg, D.; Müller, W.; Pallmer, D.: Software Agents for semantic interoperability in German Smart Sensor Web. *Workshop on Military Applications of Agent Technology in ICT and Robotics*, Den Haag, 23.-24.11.04.

[SS05] Staab, S.; Studer, R.: *Handbook on Ontologies*. Berlin: Springer, 2005.