Helmut Reiser

Sicherheitsarchitektur für ein Managementsystem auf der Basis Mobiler Agenten

Herbert Utz Verlag · Wissenschaft
München

Die Deutsche Bibliothek – CIP-Einheitsaufnahme

Ein Titeldatensatz für diese Publikation ist
bei Der Deutschen Bibliothek erhältlich

Zugleich: Dissertation, München, Univ., 2001

ISBN 3-8316-0108-9

Printed in Germany

Herbert Utz Verlag GmbH, München
Tel.: 089/277791-00 – Fax: 089/277791-01

Kurzfassung

Mobile Agenten werden im IT–Management eingesetzt, um eine statische Funktionszuweisung an Komponenten durch eine dynamische Funktionsdelegierung zu ergänzen bzw. abzulösen. Mobile Agenten sind auch ein adäquates Mittel, um organisationsübergreifende, flexible und dynamische Managementsysteme aufzubauen. Die Sicherheitseigenschaften dieser Managementsysteme spielen die entscheidende und kritische Rolle für deren Akzeptanz. Nur wenn ein Managementsystem auf der Basis Mobiler Agenten geeignet ist, die Sicherheitspolitik eines jeden, am interorganisationalen Managementsystem beteiligten, Unternehmens auch durchzusetzen, wird das System im produktiven Betrieb eingesetzt werden.

In der Arbeit wird eine umfassende und modulare Sicherheitsarchitektur für ein domänenübergreifendes Managementsystem entwickelt. Dazu wird ein abstraktes Systemmodell von Managementsystemen basierend auf Mobilen Agenten abgeleitet, um auf dieser Basis eine prospektive Risikoanalyse — unabhängig von konkreten Implementierungen — durchzuführen. Ergebnis dieser Untersuchung sind Sicherheitsanforderungen, die das gesamte Managementsystem betreffen, d.h. es werden die Sicherheit des Mobilen Agenten, des Agentensystems als Laufzeitumgebung für Mobile Agenten sowie die Sicherheit des Endsystems betrachtet. Für die Realisierung der Sicherheitsanforderungen werden geeignete Mechanismen, Sicherheitskonzepte und Bausteine der modularen Architektur entwickelt und auf Basis der Mobile Agent System Architecture (MASA) implementiert.

INHALT

Kapitel 1

Einführung

Inhaltsverzeichnis

hohe Änderungsdynamik im Management

Service Provider sind heutzutage wegen der Kundenorientierung und der Konkurrenz auf den Märkten mit einer sehr hohen Änderungsdynamik konfrontiert. Die verwendeten bzw. vorhandenen IT–Infrastrukturen zeichnen sich durch sehr große Heterogenität und zum Teil auch durch Kurzlebigkeit bei den Hard– und Software–Komponenten aus. Die vom Provider realisierten Dienste müssen auf dieser, sich ständig ändernden, technischen Basis erbracht und administriert werden. Aber auch die Kunden, die mit diesen Diensten ihre eigenen Geschäfts– bzw. Produktionsprozesse vereinfachen oder aus Basisdiensten eigene Mehrwertdienste realisieren, sind dieser hohen Änderungsdynamik ausgesetzt. Damit die Kunden sich auf ihr Kerngeschäft und ihre Kernkompetenzen konzentrieren können, wird das Management von Basis– und Mehrwertdiensten ganz oder zum Teil, im Rahmen von Outsourcing, an zuliefernde Provider übertragen. Für die Managementsysteme, die in solchen Szenarien eingesetzt werden, bedeutet dies die Notwendigkeit, schnell auf geänderte Anforderungen und Umgebungen reagieren zu können. Erschwerend wirkt sich dabei aus, dass sowohl im Falle des Outsourcing als auch im Rahmen der normalen Kunden–Provider Beziehung Managementfunktionalität über organisatorische Grenzen hinweg erbracht werden muss.

Management überschreitet organisatorische Grenzen

Um eine schnelle Anpassungsfähigkeit an geänderte Anforderungen durch das Managementsystem zu ermöglichen, wurde versucht, die statischen Managementsysteme durch dynamische Konzepte zu erweitern. Management by Delegation (MbD) und das Konzept der flexiblen Agenten [Moun 97] heben die Statik der Funktionszuweisung durch dynamische Funktionsdelegierung auf. Ein flexibler Agent kann zur Laufzeit um zusätzliche Funktionalität erweitert werden. In den letzten Jahren hat man dieses Konzept — in der noch allgemeineren Form des Mobilen Agenten — im Management eingesetzt. Ein **Mobiler Agent (MA)** ist ein flexibler Agent, der um die Fähigkeit der Migration bzw. der Mobilität erweitert wird. Ein **Multi–Hop MA** kann eine Menge von (heterogenen) Systemen besuchen und dort Management–Funktionen

ausführen. Im Gegensatz dazu ist ein **Single–Hop MA** nur in der Lage, eine einzige Migration vom Quell– zum Zielsystem auszuführen. Die Entscheidung über die Migration kann vom Mobilen Agenten autonom getroffen oder aber von „außen“ veranlasst werden.

1.1 Fragestellung

Sicherheit entscheidend für die Akzeptanz

Bei der Verwendung von flexiblen, verteilten Managementsystemen spielen Sicherheitseigenschaften im Hinblick auf die Akzeptanz und Anwendbarkeit der Mobilen Agenten Technologie eine entscheidende und kritische Rolle. Das Management von IT–Systemen setzt die Kontrolle über Ressourcen und den vollen Zugriff auf die zu administrierenden Systeme voraus. Die Verfügbarkeit und Durchsetzbarkeit von strengen Sicherheitseigenschaften ist für die Akzeptanz eines Managementsystems basierend auf Mobilen Agenten von entscheidender Bedeutung; das Fehlen solcher Eigenschaften führt zur völligen Ablehnung. Ein Managementsystem, das der Sicherheitspolicy eines Unternehmens widerspricht oder nicht geeignet ist diese Policy auch durchzusetzen, wird im produktiven Bereich nicht eingesetzt werden.

Das Ziel dieser Arbeit ist, die wesentlichen Beiträge zur Entwicklung von sicheren Systemen Mobiler Agenten in einer Top–Down–Analyse zu erarbeiten und in einer Sicherheitsarchitektur zusammenzufassen. Die wichtigsten Fragestellungen bzw. Teilprobleme auf dem Weg zu dieser Sicherheitsarchitektur lauten:

- Strukturierung des Problembereiches durch Modellbildung von Systemen Mobiler Agenten
- Ableitung eines Entitäten– bzw. Relationenmodells für eine modellbasierte und prospektive Risikoanalyse
- Ableitung notwendiger Sicherheitsanforderungen anhand dieser abstrakten Modelle und der Risikoanalyse
- Analyse bestehender Konzepte, inwieweit diese in der Lage sind die Sicherheitsanforderungen zu erfüllen
- Ermittlung von Sicherheitsmechanismen zur Durchsetzung der notwendigen Sicherheitsanforderungen item Spezifikation und prototypische Implementierung der Komponenten einer Sicherheitsarchitektur

1.2 Defizite existierender Lösungen

Bei existierenden MA–Systemen stehen die Realisierbarkeit und Implementierungsfragen der Basisfunktionen Mobiler Agenten im Vordergrund. Die Entwicklung ist getrieben von technischen Fragestellungen. Dies führt dazu,

dass jeder Hersteller eines MA–Systems eigene, proprietäre Konzepte implementiert und versucht diese auf dem Markt durchzusetzen. Es gibt keine oder nur marginale Spezifikations– oder Modellierungsversuche. Die verschiedenen existierenden Systeme sind inkompatibel. Es gibt auch kaum Standardisierungsbemühungen. Wegen der fehlenden Modellbildung gibt es bisher keine allgemeine Risikoanalyse für Systeme Mobiler Agenten, sondern nur Einzel– und Insellösungen für bestimmte Implementierungsklassen und nur für bestimmte Sicherheitsanforderungen (z.B. die Verschlüsselung von Mobilen Agenten während ihrer Übertragung). Wenn überhaupt Sicherheitsfragestellungen betrachtet werden, so betreffen diese Spezialgebiete.

nur Einzel– oder Insellösungen

Das am häufigsten zugrunde gelegte Szenario ist E–Commerce mit Hilfe von Mobilen Agenten. Dabei besucht der Mobile Agent stellvertretend für seinen Benutzer verschiedene Agentensysteme, um dort das billigste Produkt zu suchen und ggf. gleich zu erwerben. In diesem Anwendungsfall liegt der Fokus der wissenschaftlichen Untersuchungen naturgemäß auf dem Schutz des Mobilen Agenten vor einem böswilligen Agentensystem (vgl. z.B. [SaTs 98, Yee 97, Vign 98a, Hohl 98, SaTs 97]).

Fokussierung auf offene Szenarien, z.B. E–Commerce

Szenarien wie organisationsübergreifendes IT–Management mit Hilfe Mobiler Agenten wurden bisher kaum untersucht (außer am Rande in [BPW 98]). Die spezifischen Sicherheitsprobleme im IT–Management mit Mobilen Agenten wurden überhaupt nicht betrachtet. Der Hauptunterschied zu offenen Szenarien (wie z.B. dem E–Commerce) ist zum einen, dass die beteiligten Organisationen auch in vertraglichen Beziehungen zueinander stehen (z.B. in einer Kunden Provider Beziehung, vgl. Abschnitt 2.2.1). Zum anderen werden die Mobilen Agenten verwendet, um aktiv Systeme, Anwendungen oder Dienste zu steuern, zu konfigurieren, zu überwachen und auch abzurechnen. Für diese Aufgaben sind entsprechend sensible Rechte erforderlich.

Isolierte (Sicherheits–) Lösungen für Spezialprobleme sind für Managementsysteme nicht ausreichend. Es bedarf eines umfassenden und grundsätzlichen Sicherheitskonzeptes für Systeme, die auf Mobilen Agenten basieren oder diese einsetzen. Dabei reicht es auch nicht aus nur die Sicherheit des Mobilen Agenten zu betrachten, sondern es muss auch die Sicherheit der Laufzeitumgebung des Mobilen Agenten (Endsystem, Agentensystem) sowie der verschiedenen Organisationseinheiten betrachtet werden.

Sicherheit des Mobilen Agenten steht im Vordergrund

1.3 Vorgehensmodell und Ergebnisse

Das Vorgehensmodell und der Aufbau dieser Arbeit wird in Abb. 1.1 dargestellt.

Kapitel 2 definiert verwendete Begriffe und beschreibt einige Szenarien für den Einsatz von Mobilen Agenten im Anwendungsgebiet IT–Management. Um eine Risikoanalyse unabhängig von konkreten Implementierungen

Kapitel 2: Begriffs– und Modellbildung, Anforderungsanalyse

durchführen zu können, wird ein allgemeines Modell für Managementsysteme, die auf Mobilen Agenten basieren, vorgestellt. Es handelt sich dabei um ein generisches Modell, sodass die daraus abgeleiteten grundlegenden Anforderungen für alle Arten von Systemen Mobiler Agenten gelten. Aus einer allgemeinen, strategischen Sicherheitspolicy, dem vorgestellten Modell, dem Lebenszyklus Mobiler Agenten und den Anforderungen der Anwendungsdomäne IT–Management lassen sich Sicherheitsanforderungen ableiten.

Kapitel 3: State–of–the–Art

Kapitel 3 untersucht mit dem CORBA Security Service einen Sicherheitsstandard der für Systeme Mobiler Agenten, die auf der Kommunikationsplattform CORBA basieren, Anwendung finden könnte. Außerdem werden aktuelle und relevante Forschungsansätze analysiert.

Kapitel 4: Konzepte und Mechanismen

Im vierten Kapitel werden Sicherheitskonzepte erarbeitet und geeignete Sicherheitsmechanismen vorgestellt. Der Schutz eines Mobilen Agenten vor einem feindlichen Agentensystem ist ein bisher nicht gelöstes Problem. Für eine allgemeingültige Lösung dieses Problems kann man keine Annahmen über eine bestimmte Ablaufumgebung für Mobile Agenten machen (Stichwort: offene Systeme). In einem Managementsystem hingegen muss und kann davon ausgegangen werden, dass zwischen den beteiligten Organisationseinheiten vertragliche Beziehungen und gewisse Vertrauensverhältnisse existieren.
Es wird gezeigt, dass ein Mobiler Agent, sobald er auf ein Agentensystem migriert, diesem vollständig ausgeliefert ist. Aus dieser Tatsache und dem Einsatzszenario IT–Management wird der Ansatz des „Vertrauens durch Einbettungsbeziehung“ abgeleitet. Dieses Konzept besagt, dass ein Agentensystem bei gewissen sicherheitsrelevanten Aktionen als Stellvertreter („Prokurist“) des Mobilen Agenten auftreten muss, um die Sicherheitsanforderungen des Agenten durchzusetzen. Dieses Konzept ist aber nur anwendbar, wenn ein Vertrauensverhältnis zwischen Agentensystem und Mobilem Agenten aufgebaut werden kann. Das Trust Level Management beschäftigt sich damit, wie diese Vertrauensverhältnisse aufzubauen sind.

Im Folgenden werden die verschiedenen Sichten auf das allgemeine Modell aus Abschnitt 2.4 wieder aufgegriffen. Das Entitätenmodell wird verfeinert; es wird unterschieden zwischen statischen Teilen (Code, Programm; bezeichnet als Gattung) und dynamischen Teilen (in Ausführung befindlicher Code; bezeichnet als Instanz). Diese Unterscheidung und Explizitmachung des Gattungs– und Instanzbegriffs wurde bisher in der Literatur nicht getroffen.

Entitätenmodell

Um Entitäten (sowohl Gattung als auch Instanzen) und Rollen eindeutig identifizieren zu können, wird ein Namensschema entwickelt. Die Identifikation bezeichnet dann die Abbildung dieses Namens auf einen bestimmten Gattungstyp, eine Instanz oder eine Rolle. Die eigentliche Authentisierung ist die zweifelsfreie Feststellung, dass ein bestimmter Name zu einer bestimmten Entität gehört, d.h. es wird ein Mechanismus vorgestellt, mit dem der Name zweifelsfrei an eine Entität gebunden werden kann, und es wird gezeigt, wie diese Bindung verifiziert werden kann. Die Authentisierung ist Basis für die Zugriffskontrolle, daneben dient sie aber auch dazu, Aktionen zurechenbar

zu machen. Dazu muss es möglich sein, diejenige Rolle, oder die natürliche Person, die in dieser Rolle agiert, und damit für eine bestimmte Gattung oder Instanz verantwortlich ist, zu bestimmen. Auch für das Zurechenbarkeitsproblem wird eine Lösung vorgeschlagen.

Relationenmodell

Ausführungsrelation

Aufrufrelation

Kommunikationsrelation

Während das Entitätenmodell sich hauptsächlich mit den statischen Aspekten eines Systems Mobiler Agenten beschäftigt, betrachtet das Relationenmodell das dynamische Verhalten und die Interaktionen zwischen Entitäten. Die Ausführungsrelation beschäftigt sich mit der Ausführung einer Entität durch eine andere. Mobile Agenten werden beispielsweise von Agentensystemen ausgeführt, d.h. sie sind vollständig unter Kontrolle des ausführenden Agentensystems. Da auf einem Agentensystem auch mehrere Agenten und auch Agenten, für die verschiedene organisatorische Einheiten verantwortlich sind, ablaufen können, muss die Sicherstellung der Integrität und Vertraulichkeit zwischen Instanzen während deren Ausführung betrachtet werden. Dazu werden Fragen der Sichtbarkeit, Konzepte zur Trennung von Namensräumen sowie Sandboxing untersucht. Die Problemkreise, die unter dem Blickwinkel der Aufrufrelation betrachtet werden, sind Rechtekonzepte (Autorisierung) und die Delegation von Rechten sowie die damit zusammenhängende Durchsetzung von Rechten (Zugriffskontrolle). Die Kommunikations– und Migrationsrelation beschäftigt sich mit den Kommunikationsbeziehungen der Entitäten untereinander, sowie mit der Migration von Mobilen Agenten als einem „Spezialfall“ der Kommunikation. Es wird gezeigt, wie der Agent mittelbar durch das Agentensystem seine gewünschten Sicherheitseigenschaften und –anforderungen im Hinblick auf Migration und Kommunikation erreichen kann. Daneben werden Verfahren und Mechanismen vorgestellt, um die Vertraulichkeit und Integrität sowohl der Kommunikation als auch der Mobilen Agenten während der Migration zu gewährleisten. Dabei wird zwischen privaten und öffentlichen Daten des Mobilen Agenten unterschieden, die veränderbar oder unveränderlich sein können. Für alle Klassen von Daten, die ein Mobiler Agent während seiner „Reise“ transportiert, werden Verfahren zur Sicherung der Integrität und Vertraulichkeit angegeben.

Kapitel 5 + 6: Spezifikation und prototypische Implementierung der Sicherheitsarchitektur

In Kapitel 5 wird untersucht, welche Entität (Endsystem, Agentensystem oder Mobiler Agent) am besten geeignet ist, um die Sicherheitsdienste zu realisieren. Dann werden die Sicherheitskonzepte und –mechanismen zu einer Sicherheitsarchitektur vereinigt und die Komponenten dieser Architektur (CA, Authenticator, Laufzeitumgebung, Migration Manager, Communication Manager, Permission Manager, Integrity Manager und Naming Manager) spezifiziert und modelliert.

Kapitel 6 stellt dann eine prototypische Implementierung der in Kapitel 5 entwickelten Architektur vor. Als Agentensystem wird die Mobile Agent System Architecture (MASA) [GHR 99, KRRV01] verwendet und gezeigt, wie sich die spezifizierten Verfahren mit der Sprache Java und der Middleware CORBA realisieren lassen.

Die Ergebnisse der Arbeit werden in Kapitel 7 zusammengefasst und zukünftige und weiterführende Forschungsfragestellungen angegeben.

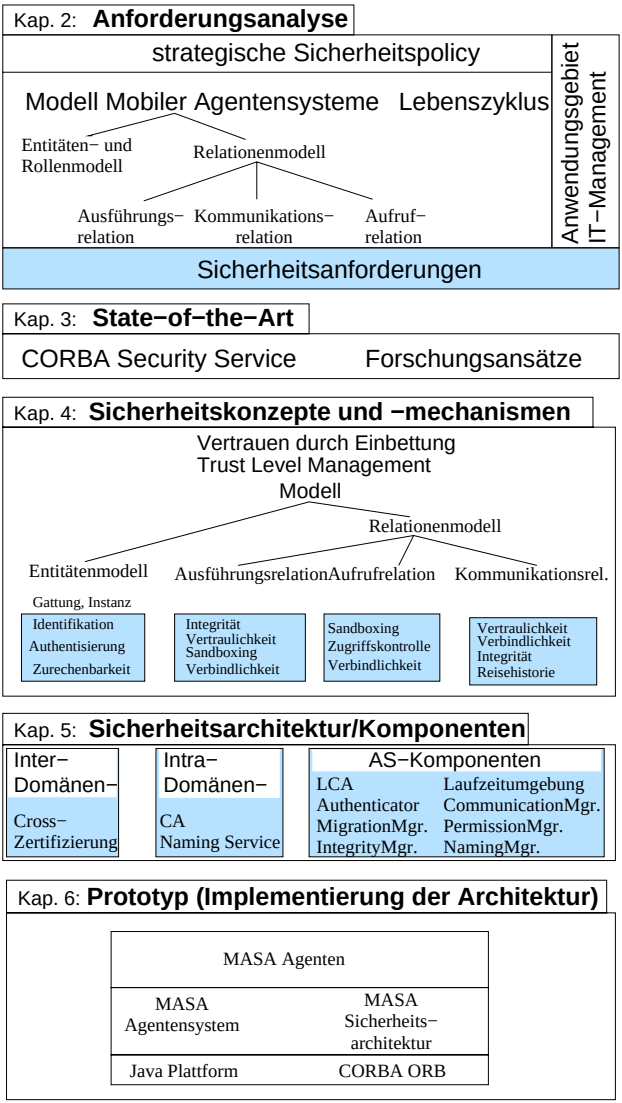

Abbildung 1.1: Vorgehensmodell; Aufbau der Arbeit

Kapitel 2

Problembeschreibung und Anforderungsanalyse: Mobile Agenten im IT–Management

Inhaltsverzeichnis