

Ein dezentrales Agentensystem unter Berücksichtigung von mehrseitiger Sicherheit

Dissertation

zur Erlangung des akademischen Grades eines
Doktors der Naturwissenschaften
(Dr. rer. nat.)
des Fachbereichs Informatik
der FernUniversität-Gesamthochschule
in Hagen

von
Dirk Westhoff
Hagen 2000

Berichte aus der Kommunikationstechnik herausgegeben von
Prof. Firoz Kaderali

Band 6

Dirk Westhoff

**Ein dezentrales Agentensystem unter
Berücksichtigung von mehrseitiger Sicherheit**

Shaker Verlag
Aachen 2000

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Westhoff, Dirk:

Ein dezentrales Agentensystem unter Berücksichtigung von
mehrseitiger Sicherheit / Dirk Westhoff.

Aachen : Shaker, 2000

(Berichte aus der Kommunikationstechnik herausgegeben
von Prof. Firoz Kaderali ; Bd. 6)

Zugl.: Hagen, Univ., Diss., 2000

ISBN 3-8265-8117-2

Copyright Shaker Verlag 2000

Alle Rechte, auch das des auszugsweisen Nachdruckes, der auszugsweisen
oder vollständigen Wiedergabe, der Speicherung in Datenverarbeitungs-
anlagen und der Übersetzung, vorbehalten.

Printed in Germany.

ISBN 3-8265-8117-2

ISSN 1437-7497

Shaker Verlag GmbH • Postfach 1290 • 52013 Aachen

Telefon: 02407 / 95 96 - 0 • Telefax: 02407 / 95 96 - 9

Internet: www.shaker.de • eMail: info@shaker.de

Danksagung

Die vorliegende Arbeit entstand während meiner Tätigkeit als wissenschaftlicher Angestellter am Lehrgebiet Praktische Informatik II des Fachbereichs Informatik der FernUniversität Gesamthochschule in Hagen.

Mein besonderer Dank gilt Herrn Prof. Dr. Claus Unger für die Diskussionen, wertvollen Hinweise und die Unterstützung bei der Durchführung dieser Arbeit. Herrn Prof. Dr. Firoz Kaderali danke ich für die Übernahme des Korreferates und seinem Interesse an der Arbeit.

In meinen Dank beziehe ich ebenfalls meine netten Kollegen am Lehrstuhl Praktische Informatik II ein. Zahlreiche - über die wissenschaftlichen Tätigkeiten hinausgehenden - Gespräche trugen zu einer unvergessenen Arbeitsatmosphäre bei.

Auch möchte ich mich bei einigen ehemaligen und gegenwärtigen Angestellten des Lehrgebiets Kommunikationssysteme für ihre offene und zuvorkommende Art bedanken mit der sie mir des öfteren beratend zur Seite standen. Es entstanden teilweise freundschaftliche Verbindungen.

Mein abschließender Dank gilt meinen lieben Eltern, ohne deren Aufmunterung und Unterstützung meine Ausbildung letztlich nicht möglich gewesen wäre.

Hagen im Oktober 2000

Für Jutta

Inhaltsverzeichnis

1	Einleitung	1
2	Grundlagen	5
2.1	Eigenschaften mobiler Agenten	5
2.2	Arbeitsumgebung mobiler Agenten	8
2.3	Basisprotokolle	9
2.3.1	Remote Procedure Call	10
2.3.2	Remote Programming	11
2.4	Mobilität und Kommunikation	12
2.4.1	Mobilität	12
2.4.2	Kommunikation	14
2.4.2.1	Direkte Kommunikation	15
2.4.2.2	Indirekte Kommunikation	16
2.5	Arbeiten auf dem Gebiet mobiler Agenten	18
2.5.1	Aglets	18
2.5.2	D'Agents	19
2.5.3	Mole	21
2.5.4	JAE	22
2.5.5	Weitere Systeme	23
2.5.6	Zusammenfassung und Motivation	23
3	Funktionsorientierter Entwurf	27
3.1	Bausteine	29
3.1.1	Der Kontext	29
3.1.1.1	Die Kontext-IP-Liste	29
3.1.1.2	Die Thread-Liste	31
3.1.2	Der Agent	32

	3.1.2.1	Das Profil	33
	3.1.2.2	Der Binärcode	34
	3.1.2.3	Die Route	35
	3.1.2.4	Die mobilen Daten	36
	3.1.2.5	Das Logbuch	37
	3.1.3	Begriffsbildung	37
3.2		Konzepte des Agenten	38
	3.2.1	Individualisierung des Agenten	38
	3.2.2	Mobilität des Agenten	41
		3.2.2.1 Migration	41
		3.2.2.2 Persistenzbildung	43
		3.2.2.3 Externalisation	44
	3.2.3	Transaktionskonzept des Agenten	45
		3.2.3.1 Transaktionsmanager	47
		3.2.3.2 Systemeigene Transaktionen	47
		3.2.3.3 Fehlerfreies Überführen und eindeutiges Lokalisieren	48
		3.2.3.4 Recovery nach einem Fehler im Zielkontext	49
		3.2.3.5 Recovery nach einem Verbindungsabbruch	52
		3.2.3.6 Recovery nach einem Fehler im Ursprungskontext	53
		3.2.3.7 Applikationseigene Transaktionen	54
3.3		Konzepte der Kontexte	54
	3.3.1	Das duale Agentensystem	55
	3.3.2	Migration bei temporärer Netzverbindung	57
		3.3.2.1 IP-Anpassung durch rückwärtigen Route-Durchlauf	58
		3.3.2.2 Erreichbarkeit des Agenten	63
	3.3.3	Das Agenten-Paradigma zur dezentralen Verwaltung	66
		3.3.3.1 Ein Verwaltungs-Agent	67
		3.3.3.2 Konsistenz und Stabilität der dezentralen Verwaltung	73
3.4		Kommunikation	82
	3.4.1	Direkte Kommunikation	83
		3.4.1.1 Kommunikation initialisieren	83
		3.4.1.2 Kommunikation durchführen	85
		3.4.1.3 Kommunikation aufheben	86
	3.4.2	Indirekte Kommunikation	86
		3.4.2.1 Dienstexport	87
		3.4.2.2 Dienstimport	87
		3.4.2.3 Dienstpflege	90

4	Sicherheit	91
4.1	Kryptographische Dienste	93
4.1.1	Klassische kryptographische Verfahren	93
4.1.1.1	Ein symmetrisches Verfahren: DES	93
4.1.1.2	Ein asymmetrisches Verfahren: RSA	95
4.1.1.3	Ein Hashverfahren: SHA	96
4.1.2	Klassische kryptographische Protokolle	97
4.1.2.1	Schlüsselaustausch nach Diffie und Hellmann	97
4.1.2.2	Byzantinische Übereinkunft	98
4.1.2.3	Nicht abstreitbarkeits-Protokolle	99
4.1.3	Mobile kryptographische Dienste	99
4.1.3.1	Aufdecken von Manipulationen: Detection Objects	100
4.1.3.2	Ausführung verschlüsselter Funktionen: EEF	100
4.2	Funktionalität des Trust-Centers	101
5	Sicherheitsorientierter Entwurf	103
5.1	Problemanalyse	104
5.1.1	Integrationsparameter	104
5.1.2	Schutzziele	106
5.1.3	Begriffsbildung	107
5.1.4	Potentielle Angriffe	108
5.1.5	Klassifizierung von Sicherheitsdiensten	111
5.1.6	Postulierte Sicherheitsdienste	112
5.1.7	Kostenfunktionen	114
5.1.8	Kryptographische Funktionen	115
5.1.8.1	Konzelations- und Signaturfunktionen	115
5.1.8.2	Hashfunktion	116
5.2	Schutz des Agenten im Netz	117
5.2.1	Ein hybrides Verfahren	117
5.2.2	Analyse	119
5.2.3	Kosten und Nutzen	121
5.3	Schutz des Kontexts vor Agenten	122
5.3.1	Rechte auf das Dateisystem	125
5.3.2	Gruppenbildung	126
5.3.3	Ausführungsrechte eines Agenten	127
5.3.4	Effektive Rechte eines Agenten	128
5.3.5	Ablauf	131

5.3.6	Datenrestauration und Protokollierung	133
5.3.7	Kosten und Nutzen	135
5.4	Schutz des Agenten vor Arbeitskontexten	136
5.4.1	Klassifizierung der Objekte des Agenten	137
5.4.2	Partieller Schutz der Route	138
5.4.2.1	Atomar verschlüsselte und signierte Route	139
5.4.2.2	Atomar verschlüsselte, verschachtelt signierte Route	143
5.4.2.3	Verschachtelt verschlüsselte, atomar signierte Route	145
5.4.2.4	Verschachtelt verschlüsselte und signierte Route	147
5.4.2.5	Koalitionen böswilliger Arbeitskontexte	148
5.4.2.6	Diskussion	152
5.4.2.7	Erweiterung der initialen Route	152
5.4.2.8	Integration	155
5.4.2.9	Kosten und Nutzen	156
5.4.3	Partieller Schutz der mobilen Daten	157
5.4.3.1	Eingabedaten	158
5.4.3.2	Temporär- und Ergebnisdaten	167
5.4.3.3	Koalitionen böswilliger Arbeitskontexte	169
5.4.4	Partieller Schutz des Binär-codes	169
5.4.4.1	Ein einfaches, prüfsummenbasiertes Protokoll	170
5.4.4.2	Prüfsummenbasiertes Protokoll mit Schiedskontext	172
5.4.4.3	Nicht abstreitbarkeits-Protokoll mit Schiedskontext	178
6	Abschließende Betrachtungen	187
6.1	Zusammenfassung	187
6.2	Ausblick	190
A	ALOHA	193
B	Kryptographische Hilfsmittel	201
C	Signaturgesetzgebung	207
	Literaturverzeichnis	209

Zur Beschreibung des Agentensystems und seiner Sicherheitsdienste sind folgende Notationen von Bedeutung:

Mengen-Notationen

\emptyset	leere Menge
\in	ist Element von
\subseteq	ist Teilmenge von
\cup	Vereinigungsmenge
\cap	Schnittmenge
$card(A)$	Kardinalität der Menge A

Logik-Notationen

\Rightarrow	daraus folgt
$:=$	wird definiert als
\exists	Existenzquantor
\forall	Allquantor
\wedge	Und-Verknüpfung
\vee	Oder-Verknüpfung

Agentensystem-Notationen

A	Agent
k	Kontext
k^X	Kontext ist Teil der Route-Erweiterung eines Agenten
q	Quellkontext
S	Schale
\mathcal{K}	Kern
$r(\mathcal{X})$	Route mit Etappen aus $\mathcal{X} \subseteq (\mathcal{S} \cup \mathcal{K})$
r^X	Route-Erweiterung
\mathcal{A}	Menge von Agenten
\mathcal{AS}	Agentensystem

Kryptographie-Notationen

e, p	öffentlicher, privater Konzelationsschlüssel asymmetrischer Verfahren
s	geheimer Konzelationsschlüssel symmetrischer Verfahren
E	Konzelationsfunktion
S	Signaturfunktion
H	Hashfunktion
$\dot{x}, \ddot{x}, \tilde{x}$	Täter, Mittäter, Verdächtiger
$\dot{x} \xrightarrow{z} y$	Angriff von \dot{x} auf y zur Verletzung des Schutzziels z
$\dot{x}, \ddot{x} \xrightarrow{z} y$	koalierender Angriff von \dot{x} und \ddot{x} auf y zur Verletzung des Schutzziels z

Rechte-Notationen

C	Komponente (Datei oder Verzeichnis) eines Dateisystems
$\mathcal{R}_k(C)$	Zugriffsrechte des Eigentümers von Kontext k auf C
$\mathcal{R}_A^{eff}(C)$	effektive Zugriffsrechte von A auf C
$\mathcal{R}_A^{exp}(C)$	explizite Zugriffsrechte von A auf C

Sonstiges

$ a $	Größe eines Datums in Bit a
$card(a)$	Anzahl der Elemente eines Datums a
$a b$	Konkatenation zweier Daten a, b
$a \text{ div } b$	ganzzahlige Division