

Dipl.-Inf. Reinhard Heite, Heidelberg

Geschützte Objektrefe- renzen und dynamische Typisierung in verteilten heterogenen Systemen

Reihe **10**: Informatik/
Kommunikationstechnik Nr. **414**

Inhaltsverzeichnis

1	Einleitung	1
1.1	Ziele der Arbeit	2
1.2	Vorgehensweise	3
2	Verteilte heterogene Objektsysteme	5
2.1	Abstraktes Objektmodell	5
2.2	Konkretes Objektmodell	7
2.3	Der Fernaufruf	8
2.4	Komponenten und Laufzeitstrukturen entfernter Objekte	10
2.4.1	Proxy-Objekte	11
2.4.2	Komponenten einer Objektimplementierung	12
2.4.3	Objektdispatching	14
2.4.4	Objekterzeugung im Server	15
2.5	Spezifikation von Objektschnittstellen	17
2.5.1	Elemente einer IDL	18
2.5.2	Netzwerkformat	23
2.5.3	Sprachabbildung	24
2.5.4	Sprachabbildung von Objekttypen	27
2.6	Systemobjekte	34
2.6.1	Namensdienst	35
2.7	Zusammenfassung	37
3	Dynamische Typkonzepte	39
3.1	Motivation	39
3.2	Dynamische Typkonzepte in der IDL	42
3.2.1	Typvariablen und dynamisch getypte Parameter	42
3.2.2	Typausdrücke	43

3.2.3	Namensbehandlung innerhalb eines Typausdrucks	45
3.2.4	Objekte mit dynamisch getyptem Zustand	47
3.2.5	Parametrisierte Typen	48
3.2.6	Dynamisch getypte Objektreferenz-Parameter	50
3.2.7	Subtyp-Beziehungen	54
3.3	Stubstrukturen für die dynamische Typisierung	59
3.3.1	TypeCodes	60
3.3.2	Dynamisches Marshalling basierend auf TypeCodes	65
3.4	Sprachabbildung von Typvariablen und dynamisch getypten Parametern	68
3.4.1	Eingabeseite	68
3.4.2	Ausgabeseite	73
3.5	Zusammenfassung	76
4	Ein Sicherheitsmodell	77
4.1	Authentisierung in verteilten Systemen	81
4.1.1	Kryptografische Basiskonzepte	82
4.1.2	Authentisierung basierend auf asymmetrischen Schlüsseln	85
4.1.3	Authentisierung basierend auf symmetrischen Schlüsseln	87
4.2	Privilegien-Attribute von Subjekten	91
4.2.1	Privilegien-Server	92
4.3	Zugriffskontrolle und Autorisierung	94
4.3.1	Die ACL-Struktur	95
4.3.2	Zugriffskontrolle	96
4.3.3	Autorisierung	96
4.3.4	Administrationsrechte assoziiert mit einem Objekt	97
4.4	Delegation	98
4.4.1	Delegations-Privilegien	102
4.4.2	Authentisierung eines Delegierten	102
4.4.3	Delegation basierend auf asymmetrischen Schlüsseln	103
4.4.4	Delegation basierend auf symmetrischen Schlüsseln	107
4.4.5	Abgeschwächte Authentisierung eines Delegierten	108
4.4.6	Delegation in einem Multi-Zellen-Szenarium	109
4.4.7	Zugriffskontrolle für Delegierte	110
4.5	Geschützte Referenzweitergabe	114

4.6	Zusammenfassung	116
5	Integration des Sicherheitsmodells	118
5.1	Authentisierter Objektaufruf	119
5.1.1	Assoziierung zwischen Subjekt und Prozeß	119
5.1.2	Anforderung des Privilege-Server-Ticket	120
5.1.3	Übermittlung des Privilege-Server-Ticket	121
5.1.4	Sichere Kanäle verschiedener Qualitäten	122
5.2	Integrierte Zugriffskontrolle und Autorisierung	123
5.2.1	Erweiterung des Server-Laufzeitsystems	124
5.2.2	Autorisierungs-Operationen	125
5.2.3	Ein ACL-Cache	126
5.2.4	Zugriffskontrolle für dynamische Objekte	128
5.3	Integration der geschützten Referenzweitergabe	129
5.3.1	Ticket-basierte Realisierung	130
5.3.2	Anmelde-basierte Realisierung	136
5.3.3	Widerruf auf der Anwendungsebene	139
5.3.4	Geschützte Referenzweitergabe und Garbage Collection	140
5.3.5	Kriterien für den Einsatz der beiden Realisierungen	141
5.4	Sprachabbildungen für die integrierte Sicherheit	141
5.4.1	Sprachabbildung von Objektreferenz-Parametern	142
5.4.2	Zugriffskontrolle innerhalb der Anwendung	144
5.5	Zusammenfassung	146
6	Zusammenfassung und Ausblick	147
A	Format der TypeCodes	150
A.1	TypeCodes für Basistypen	150
A.2	TypeCodes für zusammengesetzte Typen	150
A.2.1	Spezielle Typindikatoren	152
A.2.2	TypeCodes für Strukturen	153
A.2.3	Beispiel: TypeCodes für Typvariablen und dynamisch getypte Parameter	153
A.2.4	Beispiel: TypeCode einer Union	153
B	Dynamische Marshall-Operationen	154

B.1	Dynamisches Marshalling von Basistypen	154
B.2	Dynamisches Marshalling von zusammengesetzten Typen	155
B.2.1	Dynamisches Marshalling von Tupeln	155
B.2.2	Dynamisches Marshalling von Arrays	155
B.2.3	Dynamisches Marshalling von Unions	156
B.2.4	Operationen für die Zeigerkonstrukturen	157
B.2.5	Typvariablen und dynamisch getypte Parameter	157
B.2.6	Dynamisches Marshalling eines benannten Datentyps	158
C	Schnittstellen für die Eingabe und Ausgabe von dynamisch getypten Werten	159
C.1	InAny	159
C.2	OutAny	160
C.3	DynTyp	161