

Inhaltsverzeichnis

I. Einführung	1
1. Motivation	2
1.1. Zugriffskontrolle	4
1.2. Referenzmonitor	5
1.3. Anforderungen	5
1.4. Beitrag dieser Arbeit	9
2. Überblick über die Arbeit	11
3. Verwandte Arbeiten zur Absicherung von Servern	12
3.1. Firewalls	12
3.2. Abbildung der Sicherheitsanforderungen auf Subsysteme	15
3.3. Manuelle Einbettung von Sicherheitsfunktionalität	19
3.4. Sprachbasierte Sicherheit	19
II. Sicherheitsaspekte bei der Serverentwicklung	22
4. Überblick	23
5. Erläuterung des Begriffs Server	24
6. Security Engineering	28
6.1. Analyse der Sicherheitsanforderungen	29
6.2. Sicherheitsmodelle	30
6.3. Elemente der Sicherheitsarchitektur	34
6.4. Prinzipien für die Entwicklung sicherer Systeme	36
6.5. Vermeidung von Schwachstellen in der Implementierung	39
7. Synthese: OO-Softwareentwicklung und Security Engineering	41
7.1. OO-Softwareentwicklung	41
7.2. Zusammenführung von Software Engineering und Security Engineering	43

7.3. Konträre Anforderungen bei der Entwicklung	45
7.4. Abschließendes Beispiel	46
III. Authorization Tags	53
8. Überblick	54
9. Modell	56
9.1. Separation of concerns	56
9.2. Begriffsdefinitionen	58
9.3. Abstraktes Modell für die Zugriffskontrolle	61
10. Ablaufumgebung VSN	64
10.1. Überblick	64
10.2. Module des VSN-Servers	65
10.2.1. Tunnelmodul	66
10.2.2. VSN-Controller	67
10.2.3. Kontextserver	68
10.2.4. PDP-Prototyp	70
10.3. VSN-Programmierschnittstelle	76
10.4. Verwandte Arbeiten zur Ablaufumgebung	78
11. Sprachkonstrukte	79
11.1. Authorization Tags	79
11.2. Erweiterung der Java-Syntax	80
11.3. Gültigkeitsregeln	84
11.4. Überprüfung der Gültigkeitsregeln	88
11.5. Laufzeiteigenschaften der neuen Sprachkonstrukte	90
11.6. Alternative Implementierungsansätze	93
11.7. Verwandte Arbeiten zu sprachbasierter Sicherheit	97
11.7.1. Selective Exports	97
11.7.2. Design by Contract	97
11.7.3. Code Rewriting	98
11.7.4. Aspektorientierte Programmierung	98
12. Softwareentwicklung mit Authorization Tags	100
12.1. Von Basistags zu Benutzeroperationen	100
12.2. Integration und Betrieb von Servern	104
12.3. Beispielanwendung	106
13. Implementierung des Präprozessors	112
13.1. Parser	112
13.2. Quelltextanalyse	115
13.3. Überprüfung der Gültigkeitsregeln	117

13.4. Quelltexttransformation	119
IV. Bewertung und Ausblick	121
14. Bewertung	122
14.1. Bewertungskriterien	122
14.2. Testfälle	123
14.3. Analyse mit OO-Softwaremetriken	128
14.4. Performanceanalyse	132
14.5. Vergleich der Ansätze	135
15. Ausblick	137
15.1. Schlußbetrachtung	137
15.2. Mögliche Erweiterungen	137
V. Anhang	141
16. Java Sicherheitsarchitektur	142
16.1. Sicherheitsmerkmale von Java	143
16.2. Java Sandbox	144
16.3. Java Authentication and Authorization Service (JAAS)	149
16.4. Vergleich von JAAS und Authorization Tags	152
16.5. Verbleibende Problembereiche	153
17. Implementierung der Laufzeitumgebung	155
17.1. VSN-Controller	155
17.2. TCP/IP-Verarbeitung	157
18. Durchführung der Leistungsmessung	162
18.1. Versuchsaufbau	162
18.2. Ergebnisse	164
19. Acronymverzeichnis	166
20. Glossar	170
Abbildungsverzeichnis	176
Tabellenverzeichnis	178
Literaturverzeichnis	180