

Inhaltsverzeichnis

Verzeichnis der Abbildungen und Tabellen	XVII
Verzeichnis der Abkürzungen und Bezeichner	XIX
Verzeichnis der Definitionen und Spezifikationen	XXV
1 Einleitung	1
1.1 Mobile Software-Agenten und Bezahlssysteme für mobile Software-Agenten ..	1
1.2 Host-getriebenes Double Spending als Ausprägung des Malicious-Host-Problems	4
1.3 Zielstellung und Aufbau der Arbeit	6
2 Bezahlssysteme für mobile Software-Agenten in offenen Systemen	9
2.1 Mobile Software und mobile Software-Agenten	9
2.1.1 Ausprägungen und Definition	9
2.1.2 Anwendungsfelder des Mobile-Agent-Paradigmas	12
2.1.3 Potenziale und Herausforderungen des Mobile-Agent-Paradigmas	14
2.1.4 Sicherheitsrisiken innerhalb des Mobile-Agent-Paradigma	16
2.1.5 Modellbildung von Systemen mobiler Agenten	19
2.2 Offenheit von Systemen mobiler Software-Agenten	22
2.2.1 Erörterung des Offenheitsbegriffs	22
2.2.2 Definition offener Systeme mobiler Agenten	25
2.3 Konventionelle, elektronische und Bezahlssysteme für mobile Agenten	27
2.3.1 Reale Bezahlssysteme	27
2.3.1.1 Geld, Geldfunktionen und Zahlungssysteme	27
2.3.1.2 Die technischen Eigenschaften von Bargeld	29
2.3.2 Elektronische Bezahlssysteme	30
2.3.2.1 Definition und Modell	30
2.3.2.2 Typen und Eigenschaften	32
2.3.2.3 Münzbasierte Offline-Micropayment Systeme – Charakteristika und Lösungsansätze	35
2.3.3 Bezahlssysteme für mobile Software-Agenten in offenen Systemen	36

3	Problemanalyse und Stand der Forschung	39
3.1	Anforderungen an Mikro-Bezahlsysteme für mobile Software-Agenten	39
3.1.1	Anforderungen an elektronische Bezahlssysteme	39
3.1.2	Allgemeine Anforderungen an Mikro-Bezahlsysteme für mobile Agenten	41
3.1.3	Formen des Double Spending in Mikro-Bezahlssystemen für mobile Agenten	44
3.1.4	Zuordnungsbezogene Anforderungen an Mikro-Bezahlssysteme im Kontext des Host-getriebenen Double Spending	47
3.2	Stand der Forschung: Lösungsansätze für Host-getriebenes Double Spending	50
3.2.1	Strukturierungs- und Bewertungsschema	50
3.2.2	Software-basierte Ex-ante-Ansätze auf der Basis von Mobile Cryptography	52
3.2.3	Hardware-basierte Additive für Mobile-Cryptography-Ansätze	55
3.2.4	Software-basierte Ex-ante-Ansätze auf der Basis von Code Obfuscation	59
3.2.5	Hardware-basierte Additive für Code-Obfuscation-Ansätze	62
3.2.6	Software-basierte und Hardware-additive Ex-ante-Ansätze auf der Basis von Environmental Key Generation	63
3.2.7	Ex-ante-Ansätze auf Basis von internen Hardwareerweiterungen	65
3.2.8	Software-basierte und Hardware-additive Ex-post-Ansätze auf der Basis von Referenzzuständen	67
3.2.9	Software-basierte Ex-ante-Ansätze auf der Basis der Delegation von Signaturen	72
3.2.10	Explizite Hardware-additive Ex-ante-Ansätze auf der Basis von Threshold Schemes	73
3.3	Zusammenfassende Beurteilung der Lösungsansätze	78
4	Rechnungssysteme zur Kontrolle und Nachverfolgung von Werteflüssen	81
4.1	Systeme des Rechnungswesens in der wissenschaftlichen Betrachtung	81
4.1.1	Untersuchungsobjekt „Systeme des Rechnungswesens“	81
4.1.2	Buchhaltungs- und Rechnungs(wesen-)theorie(n)	84
4.1.3	Kontentheorien, Konten und Kontensysteme	87
4.2	Eine Axiomatik-basierte Theorie des Rechnungswesens	91
4.2.1	Wesen und Charakteristika axiomatischer Systeme	91
4.2.2	Betrachtungsgegenstand und Zielsetzung der Theorie des Rechnungswesens nach Mattessich	92

4.2.3	Axiome und Definitionen der Theorie des Rechnungswesens nach Mattessich	93
4.3	Ein Modell von auf der Doppik aufbauenden Kontensystemen.....	97
4.3.1	Terminologische, konzeptionelle und formale Basis.....	97
4.3.2	Modellierung von Kontensystem-Zuständen.....	97
4.3.3	Zustandsveränderungen von Kontensystemen.....	103
4.4	Eignung und Voraussetzungen für eine Übertragung	104
4.4.1	Eignungsprüfung.....	104
4.4.2	Methodische Vorgaben	106
4.4.3	Einordnung der methodischen Vorgaben in das Gesamtverfahren	109
5	Grobentwurf eines Mikro-Bezahlsystems für mobile Agenten.....	113
5.1	Ausgangsüberlegung und Entwurfsentscheidungen.....	113
5.1.1	Ausgangsüberlegung.....	113
5.1.2	Vorgehensmethode.....	116
5.1.3	Verwendeter Modellbildungsansatz.....	117
5.1.3.1	Modellarchitektur	117
5.1.3.2	Terminologische und konzeptionelle Basis.....	118
5.1.3.3	Formale Basis der Modellbildung	120
5.2	Formale Spezifikation ausgewählter Anforderungen.....	124
5.2.1	Anforderungsauswahl und Übersicht.....	124
5.2.2	Modellierung von Bezahlvorgängen in offenen Systemen mobiler Agenten.....	125
5.2.2.1	Zustandsmodellierung	125
5.2.2.2	Zustandsveränderungen.....	129
5.2.3	Adressierte funktionale Anforderungen an einen Grobentwurf.....	137
5.2.3.1	Zuordnungsfunktionalität	137
5.2.3.2	Detektionsmechanismus.....	139
5.3	Grobentwurf einer kontenbasierten Mikro-Bezahlsystem-Lösung	142
5.3.1	Identifikation des Systemzwecks und des abzubildenden Datums.....	142
5.3.2	Wahl der Kontenreihen-Perspektiven und der Grundgleichung des Kontensystems	144
5.3.3	Konteneinträge und Kontentypen	148
5.3.4	Kontenführung und Kontensystemzustände	156
5.3.5	Spezifikation der Buchungsvorschriften.....	159
5.3.5.1	Aktualisierung des Kontensystems	159
5.3.5.2	Nicht zu erfassende bzw. erfassbare Aktionen.....	160
5.3.5.3	Erfassung von Bezahlvorgängen.....	166

5.3.5.4	Erfassung von Migrationsvorgängen	167
5.3.5.4.1	Intra-Gruppen-Migrationen.....	167
5.3.5.4.2	Inter-Gruppen-Migrationen.....	170
5.3.5.5	Erfassung von Münzausgabe und -rücknahme.....	173
5.3.5.6	Erfassung von Plattform-Systemein- und -austritten	178
5.3.6	Detektionsmechanismus für Host-getriebenes Double Spending	180
6	Eigenschaften des Mikro-Bezahlungssystem-Entwurfs	185
6.1	Vollständigkeit des vorgestellten Mikro-Bezahlungssystems	185
6.2	Erfüllung der funktionalen Anforderungen	187
6.2.1	Nachweis der Existenz eines Zuordnungsmechanismus.....	187
6.2.2	Erfüllung der Detektionsanforderung	191
6.3	Erfüllung weiterer Zuordnungsanforderungen.....	198
6.3.1	Übersicht	198
6.3.2	Beständigkeit der Zuordnungen bei Migration	198
6.3.3	Austauschbarkeit und Teilbarkeit der Zuordnungen.....	199
6.3.4	Robustheit der Zuordnungen bei partiellen Systemausfällen	200
6.3.5	Nachvollziehbarkeit der Zuordnungen.....	201
6.4	Detektion sonstiger Missbräuche aus dem Malicious-Host-Problem	203
7	Eine Gestaltungsempfehlung für Feinentwürfe auf Basis des Grobentwurfs	207
7.1	Im Feinentwurf zu betrachtende Sicherheitsanforderungen.....	207
7.2	Gestaltungsempfehlung für Kontentypen.....	211
7.2.1	Konten für mobile Agenten.....	211
7.2.2	Host-Konten	213
7.2.3	Gruppen-Konten.....	215
7.2.4	Konten geldausgebender Stellen.....	217
7.3	Gestaltungsempfehlungen für Zustandsänderungen.....	217
7.3.1	Erfassung von Bezahlvorgängen.....	217
7.3.2	Erfassung von Agenten-Migrationen innerhalb einer Gruppe.....	219
7.3.3	Erfassung von Agenten-Migrationen zwischen Gruppen	221
7.3.4	Erfassung der Ausgabe von digitalen Münzen	223
7.3.5	Erfassung der Rückzahlung von digitalen Münzen	225
7.3.6	Erfassung des Gruppeneintritts von Hosts	227
7.3.7	Erfassung von Gruppenaustritten.....	228
7.3.8	Durchführung von Integritätsprüfungen zur Detektion von Double Spending.....	230

Inhaltsverzeichnis	XV
8 Zusammenfassung, Bewertung und Ausblick.....	233
8.1 Zusammenfassung.....	233
8.2 Kritische Würdigung.....	236
8.3 Ansatzpunkte für weiterführende Arbeiten	238
Anhang.....	241
Literaturverzeichnis.....	245