

Christian Breu

**Evaluation des biometrischen  
Tipperkennungsverfahrens PSYLock  
im Kontext automatisierter  
Authentisierungsverfahren**

**uni-edition**

Die Deutsche Bibliothek – CIP-Einheitsaufnahme

Autor: Christian Bureu

Evaluation des biometrischen Tipperkennungsverfahrens PSYLock im  
Kontext automatisierter Authentisierungsverfahren / Christian Breu

Berlin: uni-edition, 2004

ISBN 3-937151-13-3

**Dissertation**

zur Erlangung des Grades eines Doktors der Wirtschaftswissenschaften

eingereicht an der Wirtschaftswissenschaftlichen Fakultät der Universität Regensburg

Gedruckt auf holz- und säurefreiem Papier, 100 % chlorfrei gebleicht

Erhältlich im Buchhandel oder im Internet-Buchshop des Verlags ([www.uni-edition.de](http://www.uni-edition.de))

© uni-edition GmbH, Berlin 2004

Zehrendorfer Str. 11, D-12277 Berlin

Alle Rechte vorbehalten.

Herstellung: Schaltungsdienst Lange, Berlin

Printed in Germany

ISBN 3-937151-13-3

Informationen über den Verlag und das aktuelle Buchangebot finden Sie  
im Internet unter <http://www.uni-edition.de>

# INHALTSÜBERSICHT

<b>Kapitel 1</b>	<b><i>Wachsender Bedarf sicherer Erkennungssysteme in der Informationsgesellschaft.....</i></b>	<b>25</b>
1.1	Voraussetzung für den Erfolg von eBusiness ist das Vertrauen der Endkunden .....	25
1.2	Vorgehensweise .....	31
1.3	Möglichkeiten zur Überprüfung der Benutzeridentität .....	34
<b>Kapitel 2</b>	<b><i>Diskussion biometrischer Verfahren .....</i></b>	<b>45</b>
2.1	Grundlagen der Biometrie.....	45
2.2	Einsatzmöglichkeiten biometrischer Verfahren .....	57
2.3	Biometrische Verfahren .....	60
<b>Kapitel 3</b>	<b><i>Evaluation des biometrischen Merkmals Tippverhalten.....</i></b>	<b>79</b>
3.1	Kriterien auf Merkmalsebene.....	79
3.2	Zusammenfassung der Merkmalsebene .....	83
<b>Kapitel 4</b>	<b><i>Evaluation des Verfahrens PSYLock.....</i></b>	<b>85</b>
4.1	Das Verfahren PSYLock.....	85
4.2	Evaluation von PSYLock auf Verfahrensebene.....	104
4.3	Zusammenfassung der Verfahrensebene.....	160
<b>Kapitel 5</b>	<b><i>Evaluation des Verfahrens PSYLock auf Applikationsebene.....</i></b>	<b>163</b>
5.1	PSYLock als Passwort- und PIN-Ersatz .....	165
5.2	PSYLock als Windows-Logon und Desktopschutz .....	166
5.3	PSYLock in Signatur- und Verschlüsselungssystemen.....	192
5.4	PSYLock in der Remote Access-Authentifizierung.....	194
5.5	PSYLock-Authentifikation in Internet-Anwendungen .....	225
5.6	PSYLock als Identifikationssystem .....	230
5.7	Laufende Authentifizierung im Hintergrund.....	230
5.8	Signatur selbstverfasster Dokumente .....	236
5.9	Ergebnisse der Applikationsevaluation.....	239
<b>Kapitel 6</b>	<b><i>Zusammenfassung und Ausblick.....</i></b>	<b>243</b>
6.1	Ergebnisse der Evaluation.....	243
6.2	Nächste Schritte in der Entwicklung des Verfahrens PSYLock .....	245

# INHALTSVERZEICHNIS

<b>Abbildungsverzeichnis .....</b>	<b>XIV</b>
<b>Tabellenverzeichnis .....</b>	<b>XVI</b>
<b>Abkürzungsverzeichnis .....</b>	<b>XVII</b>

## ***Kapitel 1 Wachsender Bedarf sicherer Erkennungssysteme in der Informationsgesellschaft.....25***

1.1 Voraussetzung für den Erfolg von eBusiness ist das Vertrauen der Endkunden .....	25
1.2 Vorgehensweise.....	31
1.3 Möglichkeiten zur Überprüfung der Benutzeridentität.....	34
1.3.1 Alltägliche Authentisierungsproblematik.....	35
1.3.2 Besitzmerkmale.....	36
1.3.3 Wissensmerkmale .....	37
1.3.4 Nachteile klassischer Identifikationsverfahren.....	39
1.3.5 Biometrie als Lösung?.....	43

## ***Kapitel 2 Diskussion biometrischer Verfahren.....45***

2.1 Grundlagen der Biometrie .....	45
2.1.1 Begriffsdefinition .....	45
2.1.2 Arbeitsweise biometrischer Verfahren.....	46
2.1.3 Merkmalsauswahl .....	48
2.1.4 Personalisierung und Klassifikation.....	50
2.1.5 Verifikation und Identifikation.....	51
2.1.6 Fehlerraten .....	53
2.2 Einsatzmöglichkeiten biometrischer Verfahren.....	57
2.2.1 Kriminalistik .....	57
2.2.2 Zutrittssicherung .....	58
2.2.3 Zugangssicherung .....	59
2.2.4 Überwachung .....	59
2.2.5 Komfort und Personalisierung .....	60
2.3 Biometrische Verfahren.....	60
2.3.1 Fingerabdruckerkennung.....	62
2.3.2 Gesichtserkennung .....	65
2.3.3 Iriserkennung .....	68
2.3.4 Retinascan .....	70
2.3.5 Handgeometrie .....	71

2.3.6	Stimmerkennung .....	73
2.3.7	Unterschriftenerkennung .....	74
2.3.8	Tippverhalten .....	76
<b>Kapitel 3</b>	<b><i>Evaluation des biometrischen Merkmals Tippverhalten</i></b> .....	<b>79</b>
3.1	Kriterien auf Merkmalsebene .....	79
3.1.1	Der Kriterienkatalog .....	79
3.1.2	Kriterien des verwendeten biometrischen Merkmals .....	80
3.1.2.1	Merkmalsart .....	80
3.1.2.2	Merkmalseigenschaft .....	81
3.2	Zusammenfassung der Merkmalsebene .....	83
<b>Kapitel 4</b>	<b><i>Evaluation des Verfahrens PSYLock</i></b> .....	<b>85</b>
4.1	Das Verfahren PSYLock .....	85
4.1.1	Die allgemeine Methode .....	86
4.1.2	Version Freitext .....	92
4.1.2.1	Trainingsphase (Enrollment) .....	92
4.1.2.2	Authentifizierung .....	92
4.1.3	Version vereinbarter Festtext .....	93
4.1.3.1	Enrollment .....	94
4.1.3.2	Authentifizierung .....	94
4.1.4	PSYLock im Hintergrund .....	95
4.1.5	Empirische Ergebnisse zur Erkennungsqualität der Festtext-Version .....	96
4.1.6	PSYLock im Vergleich mit anderen Tipperkennungsver- fahren .....	102
4.2	Evaluation von PSYLock auf Verfahrensebene .....	104
4.2.1	Technisches System .....	105
4.2.1.1	Merkmalerfassung im System .....	105
4.2.1.2	Anforderungen aufgrund möglicher Einsatzorte .....	106
4.2.1.3	Sicherheitsanforderungen nach Einsatzort bzw. An- wendung .....	107
4.2.1.4	Toleranz des biometrischen Verfahrens bzw. Systems .....	108
4.2.1.5	Mobilität .....	109
4.2.1.6	Einsatzfelder .....	110
4.2.1.6.1	Zutrittsmechanismen .....	111
4.2.1.6.2	Zugriff .....	112
4.2.1.6.3	Kriminalistik .....	114
4.2.1.6.4	Weitere Einsatzfelder .....	115

4.2.1.7	Art der Überprüfung.....	116
4.2.1.8	Technische Spezifikation .....	116
4.2.1.9	Zertifizierung und Prüfzeichen.....	118
4.2.1.10	Produktausprägung.....	118
4.2.1.11	Voraussetzungen an das Trägersystem.....	119
4.2.1.11.1	Hardwarevoraussetzungen.....	119
4.2.1.11.2	Software .....	120
4.2.2	Sicherheitsqualität.....	121
4.2.2.1	Merkmalskriterien .....	121
4.2.2.1.1	Grad der Einzigartigkeit des Merkmals.....	121
4.2.2.1.2	Fehlerraten und Trennschärfekriterien .....	121
4.2.2.2	Ermittlung der Qualitätskennzahlen .....	125
4.2.2.2.1	Fehlerrate.....	125
4.2.2.2.2	Versuchsanordnung .....	126
4.2.2.2.3	Natürliche Variabilität der Referenzdaten .....	127
4.2.2.3	Qualität der Referenzdaten.....	128
4.2.2.4	Art der Erhebung der Falschakzeptanzrate.....	128
4.2.2.5	Ausspähbarkeit des Merkmals.....	129
4.2.3	Schutz des Systems vor Angriffen .....	129
4.2.3.1	Aufwand eines Angriffs .....	130
4.2.3.2	Allgemeine Systemrisiken.....	130
4.2.3.3	Beispiele für biometricspezifische Angriffsszenarien ..	136
4.2.4	Nicht-Technische Aspekte .....	136
4.2.4.1	Juristische Aspekte.....	136
4.2.4.1.1	Erfordernis einer aktive Mitwirkung des Benutzers zur Abgabe des biometrischen Merkmals ...	137
4.2.4.1.2	Möglichkeit einer unbemerkten Erhebung der biometrischen Daten.....	137
4.2.4.1.3	Informationsgehalt der biometrischen Daten.....	137
4.2.4.1.4	Rückschließbarkeit auf die hinter den biometrischen Daten stehende natürliche Person .....	138
4.2.4.1.5	Dauerhaftigkeit der Bindung zwischen biometrischen Daten und Personen .....	138
4.2.4.1.6	Ort der Speicherung der biometrischen Daten.....	139
4.2.4.1.7	Anwendbarkeit des Verfahrens im Zusammenhang mit der Digitalen Signatur.....	139

4.2.4.1.8	Speicherung des Merkmals auf Personal- ausweisdokumenten.....	140
4.2.4.1.9	Einsetzbarkeit des Merkmals zur strafrecht- lichen Verfolgung.....	140
4.2.5	Betreibersicht .....	140
4.2.5.1	Produktreife und Produktverfügbarkeit.....	141
4.2.5.2	Installation.....	141
4.2.5.3	Systembetrieb.....	142
4.2.5.4	Administrationsaufwand .....	143
4.2.5.4.1	Regelfall .....	144
4.2.5.4.2	Sonderfälle (Aufwand relativ zum Normalfall)....	144
4.2.5.5	Investitionssicherheit.....	145
4.2.5.5.1	Zukunftssicherheit .....	145
4.2.5.5.2	Abhängigkeit vom Anbieter .....	146
4.2.5.5.3	Abhängigkeit vom Technologielieferanten .....	147
4.2.5.6	Integrationsfähigkeit.....	147
4.2.5.6.1	Systemintegration .....	147
4.2.5.6.2	Lösungsintegration / Integration in das Sicher- heitskonzept.....	148
4.2.5.7	Kosten .....	149
4.2.5.7.1	Einmalige Kosten .....	149
4.2.5.7.2	Laufende Kosten.....	150
4.2.6	Benutzerakzeptanz .....	151
4.2.6.1	Informationstransparenz.....	151
4.2.6.2	Enrollment und Benutzerführung .....	152
4.2.6.3	Diskriminierungsfreier Einsatz.....	152
4.2.6.3.1	Ausgrenzung durch das verwendete Merkmal.....	153
4.2.6.3.2	Ausgrenzung aufgrund personenbezogener Besonderheiten .....	153
4.2.6.3.3	Notwendigkeit von Ersatzverfahren .....	153
4.2.6.3.4	Kosten für Nutzer .....	153
4.2.6.4	Handhabung der Verfahren .....	154
4.2.6.4.1	Einfachheit und Bequemlichkeit .....	154
4.2.6.4.2	Schnelligkeit.....	154
4.2.6.4.3	Ergonomie der Anwendergeräte.....	156
4.2.6.4.4	Übertragbarkeit von Zugangsberechtigungen im Arbeitsalltag .....	156

4.2.6.5	Bedenken und Befürchtungen .....	157
4.2.6.5.1	Physische und moralische Unversehrtheit .....	157
4.2.6.5.2	Kriminelle Handlungen Dritter und Datenmissbrauch .....	157
4.2.6.5.3	Erzwungene Nutzung .....	158
4.2.6.5.4	Nutzung für Zwecke der Strafverfolgung .....	158
4.2.6.5.5	Scheu und Scham .....	159
4.2.7	System- und Merkmalsausfall .....	159
4.3	Zusammenfassung der Verfahrensebene .....	160
<b>Kapitel 5 Evaluation des Verfahrens PSYLock auf Applikations-</b>		
<b>ebene.....</b>		<b>163</b>
5.1	PSYLock als Passwort- und PIN-Ersatz .....	165
5.2	PSYLock als Windows-Logon und Desktopschutz .....	166
5.2.1	Technische Realisierung .....	166
5.2.1.1	Windows 2000-Anmeldeverfahren.....	166
5.2.1.2	Integration des Verfahrens PSYLock in den Anmeldeprozess .....	171
5.2.1.3	Authentifizierung über SmartCard .....	176
5.2.1.4	Schutz durch Bildschirmschoner und Sperrung des Desktops.....	182
5.2.2	Vergleich mit anderen Biometrie-Verfahren.....	182
5.2.2.1	Sicherheit.....	182
5.2.2.2	Komfort .....	188
5.2.2.3	Stationäre Rechner .....	190
5.2.2.4	Mobile Rechner .....	191
5.3	PSYLock in Signatur- und Verschlüsselungssystemen .....	192
5.3.1	Technische Realisation.....	192
5.3.2	Vergleich mit anderen Biometrie-Verfahren.....	193
5.4	PSYLock in der Remote Access-Authentifizierung.....	194
5.4.1	Grundlegende Authentifizierungsverfahren .....	195
5.4.1.1	Schwache Authentifizierungsverfahren: Statische Passwörter .....	195
5.4.1.2	Schwache Authentifizierungsverfahren: Einmalige Passwörter .....	198
5.4.1.3	Starke Authentifizierungsverfahren: Challenge- Response-Verfahren .....	199
5.4.2	Remote Access Services und Virtuelle Private Netzwerke ..	204

5.4.2.1	Virtuelle Private Netzwerke .....	205
5.4.2.2	Grundlagen eines VPN .....	205
5.4.2.3	Sicherheitsmerkmale eines VPN .....	206
5.4.2.4	Elemente eines VPN .....	207
5.4.2.5	Arten von VPN-Verbindungen .....	209
5.4.2.6	Protokolle des VPN .....	210
5.4.3	Benutzerauthentifizierung mit PSYLock im VPN .....	211
5.4.4	Technische Realisation .....	215
5.4.4.1	PSYLock in MS-CHAPv2 .....	215
5.4.4.2	PSYLock in EAP-TLS mit SmartCard .....	220
5.4.4.3	PSYLock als EAP-Erweiterung: EAP-PSY .....	222
5.4.5	Vergleich mit anderen Biometrie-Verfahren .....	225
5.5	PSYLock-Authentifikation in Internet-Anwendungen .....	225
5.5.1	Authentifizierungsprotokolle im Internet .....	225
5.5.2	Technische Realisation .....	227
5.5.3	Vergleich mit anderen Biometrie-Verfahren .....	229
5.6	PSYLock als Identifikationssystem .....	230
5.7	Laufende Authentifizierung im Hintergrund .....	230
5.7.1	Technische Realisation .....	231
5.7.2	Vergleich mit anderen Biometrie-Verfahren .....	236
5.8	Signatur selbstverfasster Dokumente .....	236
5.8.1	Technische Realisation .....	237
5.8.2	Vergleich mit anderen Biometrie-Verfahren .....	239
5.9	Ergebnisse der Applikationsevaluation .....	239
<b>Kapitel 6</b>	<b>Zusammenfassung und Ausblick .....</b>	<b>243</b>
6.1	Ergebnisse der Evaluation .....	243
6.2	Nächste Schritte in der Entwicklung des Verfahrens PSYLock .....	245
<b>Anhang .....</b>		<b>249</b>
<b>Literaturverzeichnis .....</b>		<b>257</b>

## ABBILDUNGSVERZEICHNIS

<i>Abbildung 1-1: Beweggründe mittelständischer Unternehmen gegen eBusiness</i> .....	26
<i>Abbildung 1-2: Funktionsschichtenmodell biometrischer Anwendungen</i> .....	32
<i>Abbildung 1-3: Dreistufiges Evaluationsmodell biometrischer Verfahren</i> .....	34
<i>Abbildung 2-1: Aufbau biometrischer Systeme</i> .....	47
<i>Abbildung 2-2: Zusammenhang zwischen Toleranzschwelle, FAR, FRR und EER</i> .....	55
<i>Abbildung 3-1: PSYLock-Evaluationsmodell auf Merkmalsebene</i> .....	79
<i>Abbildung 4-1: PSYLock-Evaluationsmodell auf Verfahrensebene</i> .....	104
<i>Abbildung 4-2: Ergebnisse des PSYLock-Feldtests: False Acceptance Rate der Version mit Freitext</i> .....	122
<i>Abbildung 4-3: Ergebnisse des PSYLock-Feldtests: FRR der Version mit Freitext</i> .....	123
<i>Abbildung 4-4: Ergebnisse Feldtest PSYLock: FAR, FRR und EER der Festtext-Version</i> .....	124
<i>Abbildung 4-5: Allgemeine Angriffspunkte biometrischer Verfahren</i> ...	131
<i>Abbildung 5-1: PSYLock-Evaluationsmodell auf Anwendungsebene</i> ....	164
<i>Abbildung 5-2: Standard Windows 2000-Anmeldeprozess</i> .....	167
<i>Abbildung 5-3: Integrationsmodell von PSYLock in Windows 2000-Anmeldeprozess</i> .....	171
<i>Abbildung 5-4: Ablaufmodell der lokalen Anmeldeprozedur von PSYLock in Windows 2000</i> .....	173
<i>Abbildung 5-5: Ablaufmodell der Netzwerk-Anmeldeprozedur von PSYLock in Windows 2000</i> .....	175
<i>Abbildung 5-6: Integrationsmodell von PSYLock als Freischaltmechanismus für SmartCards ohne Templateablage</i> .....	178
<i>Abbildung 5-7: Integrationsmodell PSYLock als Freischaltmechanismus für SmartCards mit Templateablage</i> .....	179
<i>Abbildung 5-8: Integrationsmodell PSYLock als Freischaltmechanismus für SmartCards als „Match-On-Card“</i> .....	180

<i>Abbildung 5-9: FAR- und FRR-Ergebnisse der CESG-Studie verschiedener Biometrien mit Ergebnissen aus dem PSYLock-Feldversuch der Festtext-Version.....</i>	<i>186</i>
<i>Abbildung 5-10: Ergebnis des Feldversuchs BioTrusT: Erkennungsleistungen verschiedener Biometrien.....</i>	<i>188</i>
<i>Abbildung 5-11: Authentifizierungsverfahren mit statischem Passwort..</i>	<i>195</i>
<i>Abbildung 5-12: Authentifizierungsverfahren mit gehashtem Passwort .</i>	<i>197</i>
<i>Abbildung 5-13: Authentifizierungsverfahren nach dem Challenge-Response-Verfahren bei symmetrischer Verschlüsselung .....</i>	<i>200</i>
<i>Abbildung 5-14: Replacement-Attacke bei Challenge-Response-Verfahren und symmetrischer Verschlüsselung.....</i>	<i>201</i>
<i>Abbildung 5-15: Authentifizierungsverfahren - Challenge-Response-Verfahren bei asymmetrischer Verschlüsselung.....</i>	<i>203</i>
<i>Abbildung 5-16: Wirkungsweise eines Virtuellen Privaten Netzwerks (VPN).....</i>	<i>206</i>
<i>Abbildung 5-17: Typische Elemente eines VPN .....</i>	<i>208</i>
<i>Abbildung 5-18: Szenario eines VPN unter Verwendung eines Internet Service Providers (ISP) .....</i>	<i>209</i>
<i>Abbildung 5-19: Schematischer Ablauf einer MS-CHAPv2 Authentifizierung.....</i>	<i>215</i>
<i>Abbildung 5-20: PSYLock-Integrationsmodell in MS-CHAPv2 mit Verschlüsselungs-API und Diskette als externen Passwortspeicher .....</i>	<i>219</i>
<i>Abbildung 5-21: PSYLock-Integrationsmodell in EAP-TLS mit Templateablage in SmartCard .....</i>	<i>221</i>
<i>Abbildung 5-22: PSYLock-Integrationsmodell in EAP-TLS mit SmartCard ("Match-On-Card") .....</i>	<i>222</i>
<i>Abbildung 5-23: PSYLock-IDS-Architektur für Windows NT, 2000 und XP .....</i>	<i>234</i>
<i>Abbildung 5-24: Ergebnis des PSYLock-Evaluationsmodells .....</i>	<i>242</i>

## TABELLENVERZEICHNIS

<i>Tabelle 4-1: Ergebnisse des Feldtestes mit Festtext-Version: FAR und FRR .....</i>	<i>99</i>
<i>Tabelle 4-2: Ergebnisse des Feldtestes mit Festtext-Version: Auswertung Fragebogen Teil 1 .....</i>	<i>100</i>
<i>Tabelle 4-3: Ergebnisse des Feldtestes mit Festtext-Version: Auswertung Fragebogen Teil 2 .....</i>	<i>101</i>
<i>Tabelle 4-4: Vergleich der Erkennungsleistung verschiedener Tipperkennungsstudien.....</i>	<i>103</i>
<i>Tabelle 4-5: Ergebnisse der Tippverhaltenserkennung bei Mobiltelefonen.....</i>	<i>114</i>
<i>Tabelle 5-1: Ergebnis der Studie BioIS mit Ergebnissen aus dem PSYLock-Feldversuch mit Festtext-Version: FRRs bei variierender FRR-Konfiguration.....</i>	<i>184</i>
<i>Tabelle 5-2: Ergebnis der Studie BioIS mit Ergebnissen aus dem PSYLock-Feldversuch mit Festtext-Version: FAR und FRR nach fünften Versuch.....</i>	<i>184</i>
<i>Tabelle 5-3: Vergleich verschiedener Architekturen zur Integration von PSYLock in eine VPN-Authentifizierung .....</i>	<i>224</i>

## VORWORT

Ein steiniger und von mancher Wendung durchzogener Weg führte zu dieser meiner Dissertationsschrift. Noch unter meinem ersten Doktorvater Prof. Dr. Gerhard Niemeyer begann ich Ende 1998 mein Promotionsvorhaben am Lehrstuhl Wirtschaftsinformatik I – Kybernetik und Systemtheorie - an der Universität Regensburg. Die Ausrichtung des Lehrstuhls versprach wie schon bei meiner Diplomarbeit eine Beschäftigung mit der Thematik der Simulation und Prozessplanung und –steuerung. Gemeinsam mit dem Siegeszug des Internet und dessen Integration in den betrieblichen Wertschöpfungs- und Informationsfluss - insbesondere in global operierenden Konzernen - ergab sich die Kooperation mit einem weltweit aktiven Verpackungsunternehmen für Pharmaprodukte. Daraus erwuchs ein Projekt für eine dynamische, auf Active Server Pages und MSSQL-Server - Datenbanktechnologie basierende, Logistikplattform. Dieses sollte zugleich das Thema meiner Dissertation bereitstellen. Nach dem überraschenden Ableben meines Doktorvaters im Jahre 1999 konnte allerdings das bereits teilweise realisierte Projekt nicht mehr fortgesetzt werden. Inspiriert durch die vorangegangene Arbeit, einen befreundeten Inhaber eines Marketingunternehmens und durch die Möglichkeiten des World Wide Web kam ich zusammen mit meinem damaligen Kollegen Dr. Norbert Meckl auf die Idee, ein Projektmanagementportal für verteilte Projektgruppen mit integrierter Auftraggeberschnittstelle zu entwickeln. Unter dem Arbeitstitel WORM (We offer real modularity) entstand innerhalb der nächsten Monate unter großem Programmieraufwand ein unter Java und auf einer MySQL-Datenbank realisiertes Internetportal. Mit ihm sollten z.B. Marketingfirmen oder Fotografen ihre Arbeiten intern bearbeiten und koordinieren und gleichzeitig den Auftraggebern den aktuellen Projektfortschritt und die Zwischen- bzw.

Endergebnisse präsentieren können. Auf der Suche nach einem neuen Doktorvater bot mir Prof. Dr. Dieter Bartmann vom Lehrstuhl Wirtschaftsinformatik II für Bankinformatik und Bankstrategie seine Hilfe und Bereitschaft als Gutachter an. Zugleich empfahl er mir, meine Dissertation auf eine Arbeit seines Sohnes zu fußen, die sich mit der Entwicklung eines biometrischen Verfahrens beschäftigt. Dieses System namens PSYLock identifiziert den Benutzer auf Basis dessen Tippverhaltens. Dieses Verfahren sollte weiterentwickelt, also in seiner Güte verbessert, benutzerfreundlicher und schneller gemacht, als komfortable Windowsanwendung komfortabler umgesetzt und zu guter Letzt in einem Feldversuch getestet werden. Dieses Angebot nahm ich schließlich dankbar an. Als Resultat dieser Anstrengungen entstand während der vergangenen zweieinhalb Jahre dieses Ihnen nun vorliegende Werk. Die Arbeit an WORM wurde gleichzeitig aus Zeitgründen eingestellt. Wie viele andere „Start-Ups“ so wurde auch WORM zwar nie kommerziell erfolgreich umgesetzt, fand allerdings Eingang in mehrere Veröffentlichungen zusammen mit Dr. Norbert Meckl und Prof. Dr. Johannes Sametinger, der zeitweise die Vertretung des vakanten Lehrstuhls innehatte.

Mein Dank gilt einer Vielzahl von Personen, die mich entweder schon seit langer Zeit begleitet und unterstützt oder zum Gelingen dieser Arbeit besonders beigetragen haben. Zuallererst seien meine Eltern genannt, die meiner Ausbildung nicht nur finanziell, sondern auch immer mit Rat und Tat zur Seite standen. Gleich an zweiter Stelle möchte ich meine Freundin Kerstin nennen, die auch als Rezensent dieser Arbeit den letzten sprachlichen Schliff verlieh. Ein besonders großer Dank gebührt meinem Freund Norbert Meckl. Nicht nur dass er mich bei verschiedenen Projekten wie WORM und daraus folgende Veröffentlichungen beriet. Durch seine Erfahrung wirkte er entscheidend an der Endfassung meiner Dissertation mit. Beson-

ders in der Zeit nach dem Ableben meines ersten Doktorvaters kümmerte er sich vorbildlich um die „übrig gebliebenen“ Mitassistenten am Lehrstuhl. Gleicher Dank gilt Christine Handl, dem guten Geist und Sekretärin am neuen und alten Lehrstuhl für Wirtschaftsinformatik, für die schöne und angenehme Atmosphäre und der moralischen und leiblichen Unterstützung während der langjährigen gemeinsamen Zeit am Lehrstuhl. Akademisch gilt natürlich der erste Dank an meinem Doktorvater Prof. Dr. Dieter Bartmann, Ideengeber und Motivator für diese Arbeit, Prof. Dr. Peter Lory, meinem Zweitgutachter und Dr. Dieter Bartmann jun., auf dessen Arbeit ich aufbauen durfte und der bei technischen Problemen zumeist der erste Ansprechpartner war. Für die Bereitschaft, ihre Zeit für die Feldversuche von PSYLock zu opfern, möchte ich allen Mitarbeitern des Lehrstuhls von Prof. Bartmann und den Mitarbeitern des ibi, des Institutes für Bankinformatik, nochmals recht herzlich danken, allen voran Gabriele Matzinger für deren Bemühen um das Gelingen von PSYLock. Nicht vergessen möchte ich Prof. Dr. Günther Pernul, der in der Endphase meiner Promotion die Nachfolge von Herrn Niemeyer an meinem Lehrstuhl übernahm und mir neben der anstehenden Lehre ausreichend Gelegenheit für die Arbeit an meiner Dissertation ermöglichte.

Last but not least gilt ein großer Dank Frau Sylvia Hartmann vom uni-edition Verlag für die nette Zusammenarbeit und ihre ausdauernden und erfolgreichen Bemühungen, meine geistigen Ergüsse in eine druckbare Form zu bringen.

