

Günter Müller Martin Reichenbach (Hrsg.)

Sicherheitskonzepte für das Internet

**5. Berliner Kolloquium der
Gottlieb Daimler- und Karl Benz-Stiftung**

Mit 28 Abbildungen



Springer

Inhalt

Einleitung der Herausgeber.....	1
1 Allgegenwärtigkeit des Computers –	
Datenschutz in einer Welt intelligenter Alltagsdinge	7
1.1 Der unsichtbare Computer	7
1.1.1 Technische Grundlagen.....	8
1.1.2 Herausforderungen.....	10
1.2 Datenschutz in Ubiquitären Systemen?	11
1.2.1 Grundlagen für die Wahrung der Privatsphäre.....	13
1.2.2 Anonymität und Vertraulichkeit	14
1.2.3 Transparenz	17
1.2.4 Vertrauen und Absicherung	19
1.3 Ausblick	22
Literatur.....	26
2 Sicherheit und Vertrauen: Mehrwert im E-Commerce.....	27
2.1 Sicherheit ist „Technikfolger“	28
2.1.1 Das Mittelalter-Paradigma der Vergangenheit	28
2.1.2 Das Internet-Paradigma der Gegenwart.....	29
2.1.3 Das Allgegenwärtigkeits-Paradigma der Zukunft.....	30
2.2 Sicherheitsmechanismen ändern sich – Schutzziele bleiben.....	31
2.3 Vertrauen: Mehrwert für den Electronic Commerce .	32
2.3.1 Komplementarität zwischen mehrseitiger Sicherheit und Vertrauen im Electronic Commerce	32
2.3.2 Vertrauensgegenstände im Electronic Commerce	33
2.3.3 Vertrauensobjekte im Electronic Commerce	35
2.3.4 Transaktionen und vertrauens- generierende Aktionen	36

2.4	Vertrauensinstitutionen.....	38
2.5	Fazit	42
	Literatur	43
3	Wie sicher kann Sicherheit sein?	45
3.1	Einleitung.....	45
3.2	Das RSA-Verfahren.....	46
3.3	Ein mathematisches Problem: Faktorisieren	48
3.4	Sicherheit beweisen	51
3.5	Flexibilität.....	52
	Literatur	54
4	Vertrauen im Internet:	
	Wie sicher soll E-Commerce sein?.....	57
4.1	Zusammenfassung	57
4.2	Teil 1: Vertrauen im Internet.....	57
4.2.1	E-Commerce	57
4.2.2	Das Vertrauensproblem.....	60
4.2.3	Das Internet	62
4.2.4	Die Lücke zwischen lokaler Sicherheit und globaler Unsicherheit	65
4.3	Teil 2: Wie sicher soll E-Commerce sein?	68
4.3.1	Automat und Mensch – Intention und Interpretation.....	68
4.3.2	Vertrauen	69
4.3.3	Wittgensteins Sprachspiele.....	71
4.3.4	Ein Personen-Rollen-Akteure-Modell für Telekooperation	75
4.3.5	Risiko als Gegenstand von E-Commerce.....	83
	Literatur	85
5	FairPay: Sicherer Zahlungsverkehr im Netz	87
5.1	Abstract.....	87
5.2	Was soll FairPay?	88
5.3	Was ist FairPay?	89
5.4	Was macht FairPay?	90
5.5	Die VSE-Methodologie	91
5.6	Das VSE-System	93
5.7	Was bietet FairPay?	97
5.7.1	Formale Modellierung von Sicherheitspolitiken	98
5.7.2	Formale Entwicklung	99
5.7.3	Vorgehensmodell.....	99
	Literatur	102

6	Sichere elektronische Zahlungen durch Individuelles Risikomanagement	105
6.1	Risiken elektronischer Zahlungssysteme	105
6.2	Risiko, Risikoanalyse und Risikohandhabung.....	107
6.2.1	Der Risikobegriff	107
6.2.2	Risikoanalyse: Bewertung elektronischer Zahlungssysteme	108
6.2.3	Individuelle Risikohandhabung mit dem Virtual Internet Payment Assistant	109
6.3	Anforderungsprofile als Grundlage für die Individuelle Risikohandhabung.....	114
6.3.1	Abstrahierung der Anforderungen	114
6.3.2	Ebenenmodell für Anforderungsprofile.....	116
6.3.3	Realisierung der Anforderungsprofile mit dem Scoring-Verfahren	119
6.4	Zahlungssystemwahl mit dem Virtual Internet Payment Assistant	124
6.4.1	Bezug aktueller Zahlungssystem- und Anforderungsprofile.....	124
6.4.2	Abgleich von Zahlungssystem- und Anforderungsprofilen.....	125
6.4.3	Identifizierung des Restrisikos.....	128
6.4.4	Weitergehende Absicherung des Restrisikos	129
6.5	Lernfähigkeit des Virtual Internet Payment Assistants.....	129
6.6	Ausblick	130
	Literatur.....	133
7	Benutzbare Sicherheit - Der Identitätsmanager als universelles Sicherheitswerkzeug	135
7.1	Komplexitätsreduzierung der Benutzungsoberfläche.	136
7.1.1	Mehrseitige Sicherheit und Schutzzielimplikationen.....	136
7.1.2	Die Teil-Identität.....	138
7.2	Identitätsmanagement	139
7.2.1	Generische Einheiten	139
7.2.2	Funktionen und Eigenschaften des Identitätsmanagers	142
7.2.3	Migration des Identitätsmanagers	142
7.3	Identitätsmanagement und Schutz der Privatsphäre ..	143
7.4	Ausblick	143
	Literatur.....	145

8	„Wer ist mein Nächster?“	
	Zur Authentifikation des Kommunikationspartners	147
8.1	Grundlagen	148
8.2	Authentifikation	148
8.3	Public Key Infrastructures	152
8.4	Identität und E-Commerce	155
8.5	Schlussbemerkungen	157
	Literatur	160
9	Sicherheit im E-Commerce = Rechtssicherheit	161
9.1	Einleitung	161
9.2	Grundlegende Risiken im E-Commerce	162
9.3	Risiken und (Selbst-)Regulierung	165
9.3.1	Selbstregulierung in geschlossenen und offenen Systemen	165
9.3.2	Schutz außerhalb von bi- und multilateralen Beziehungen	170
9.3.3	Der Schutz der Identität (Datenschutz)	173
9.3.4	Globalität des Netzes	175
9.4	Recht, Sicherheit und Rechtssicherheit	177
9.5	Schluss	181
	Literatur	183
10	A Concept of Net-Community Security Based on a 3D Net-Space Model	185
10.1	Introduction	185
10.2	Net Communities and Security	186
10.2.1	Overview of BA	186
10.2.2	Immunization Work of a BA	187
10.3	The 3-Dimensional Model and Security	188
10.3.1	Code-Based Security	188
10.3.2	Symbol-Based Security	189
10.3.3	Recording-Based Security	189
10.4	Conclusion	190
11	Datenschutz und IT-Sicherheit – zwei Seiten derselben Medaille	191
11.1	Herausforderungen für den Datenschutz	191
11.2	Der Neue Datenschutz	193
11.3	Datenschutz durch Technik	195
11.4	Integrierte Sicherheitsinfrastrukturen	198
11.5	Fazit	200
	Literatur	202
	Autorenverzeichnis	205
	Index	207