

Dipl.-Wirtsch.-Inf. Ulrich Kohl, Gornheimertal

Benutzerbezogene Datensicherheit in Kommunikationssystemen

Reihe **10**: Informatik/
Kommunikationstechnik Nr. **446**

Inhaltsverzeichnis

I	Mehrseitige Sicherheit als Voraussetzung akzeptierter technisch vermittelter Kommunikation	1
I.1	Informationstechnik und Sicherheit.....	1
I.2	Aspekte und Dilemma der Sicherheit	3
I.3	Vorgehensweise und Bezug zum SaferCom-Projekt.....	5
II	Datensicherheit in offenen Kommunikationssystemen	7
II.1	Datenschutz und Datensicherheit.....	7
II.2	Mehrseitige Sicherheit als Bewertungsreferenz	9
II.3	Offene Kommunikationssysteme.....	9
II.3.1	Architekturen offener Netze	10
II.3.2	Das ISO-OSI-Referenzmodell.....	11
II.3.3	Intelligente Netze.....	14
II.4	Aspekte der Sicherheit	18
II.4.1	Grundbedrohungen	18
II.4.2	Abwehr der Bedrohungen durch IT-externe Maßnahmen.....	19
II.4.2.1	Bauliche Maßnahmen	20
II.4.2.2	Organisatorische Maßnahmen	22
II.4.2.3	Rechtliche Grundlagen	25
II.4.3	Sicherheitsanforderungen an IT-Systeme.....	26
II.4.3.1	Datenschutzrechtliche Grundlagen	26
II.4.3.2	Sicherheitsanforderungen der direkt Beteiligten	28
II.4.3.3	Anforderungen an die technische Umsetzung	28
II.4.4	Abstraktionsebenen der Sicherheit	29
II.4.4.1	Subjektive und objektive Sicherheit	30
II.4.4.2	Sicherheitsphilosophie	32
II.4.4.3	Sicherheitspolitik	32
II.4.4.4	Sicherheitsmodelle	33
II.4.4.5	Basis-Sicherheitsdienste	35
II.4.4.6	Sicherheitsmechanismen	38
II.4.4.7	Kryptologie	46
II.4.5	Sicherheitsstandards	54
II.4.5.1	ISO/OSI 7498-2	55
II.4.5.2	ECMA TR-46 und ECMA-138	57
II.4.5.3	CCITT X.500 und X.700	58
II.4.6	Sicherheitsevaluation.....	59
II.5	Grundlagen zur Architektur und Modellierung von Kommunikation	60
II.5.1	Nutzerorientierte Modellierung von Kommunikation.....	60

II.5.1.1 Menschliche Kommunikation	62
II.5.1.2 Technisch vermittelte Kommunikation	73
II.5.1.3 Sicherheitsaspekte	77
II.5.1.4 Metakommunikation der Sicherheitsanforderungen bei technischer Kommunikation	79
II.5.2 Benutzerbezogene Datensicherheit	80
III Erhebung benutzerbezogener Sicherheitsanforderungen im Krankenhaus	81
III.1 Das Fallbeispiel Klinikum Freiburg	81
III.2 Sicherheitsmerkmale aktueller Krankenhausinformationssysteme	84
III.2.1 Einsatz von Krankenhausinformationssystemen	84
III.2.2 Datenfluß und Verantwortlichkeiten	88
III.2.3 Gesetzliche Rahmenbedingungen – Folgerungen und Durchsetzung im Krankenhaus	89
III.3 Referentielle Erhebungstechnik für Sicherheitsanforderungen	92
III.3.1 Die Annahme allgegenwärtiger Information und zentraler Organisation	92
III.3.2 Fallszenarien für Krankenhausabläufe	95
III.3.2.1 Patientenaufnahme	96
III.3.2.2 Befundung	97
III.3.2.3 Inanspruchnahme einer Leistungsstelle	99
III.3.2.4 Bestellung eines Konsiliariums	100
III.3.2.5 Durchführung einer Operation (OP)	101
III.3.2.6 Stationswechsel des Patienten	102
III.3.2.7 Notfall bei Abwesenheit des verantwortlichen Arztes	103
III.3.2.8 Patientenentlassung	104
III.4 Benutzerbezogene Sicherheitsmerkmale verteilter Krankenhausinformationssysteme ..	105
IV Objektorientierte Modellierung benutzerbezogener Datensicherheit	108
IV.1 Klassifikation von Sicherheitsanforderungen in technisch vermittelter Kommunikation	109
IV.1.1 Anforderungen auf Benutzerebene	111
IV.1.1.1 Bestimmung der Elemente	112
IV.1.1.2 Kontextbezogene Spezifikationen	113
IV.1.1.3 Explizite Zustimmung	119
IV.1.1.4 Anforderungen an aktive Maßnahmen	120
IV.1.1.5 Metaanforderungen	121
IV.1.2 Anforderungen auf den Ebenen der Sicherheitsdienste und Sicherheitsmechanismen	122
IV.2 Die funktionale Nutzerschnittstelle	124
IV.2.1 Der objektorientierte Ansatz für benutzerbezogene Sicherheit	124
IV.2.1.1 Allgemeine Objektorientierung	125
IV.2.1.2 Erweiterung des objektorientierten Ansatzes	128
IV.2.2 Objektorientierte Modellierung von Kommunikation	129

IV.2.2.1 Formale Darstellung	130
IV.2.2.2 Beschreibung der objektorientierten Eigenschaften der Elemente	134
IV.2.2.3 Zusammenfassung	138
IV.3 Technische Umsetzung der Sicherheitsanforderungen	138
V Das SaferCom-Projekt und seine Eignung für benutzerbezogene Datensicherheit.....	143
V.1 Das SaferCom-Projekt	143
V.1.1 Ziel und Vorgehensweise	143
V.1.2 Entwurfsentscheidungen.....	143
V.1.3 Abgrenzung zum REMO-Ansatz	144
V.2 Die Komponenten von SaferCom und ihre Nutzbarkeit für benutzerbezogene Datensicherheit	145
V.2.1 Das offene Dokumentenarchiv	145
V.2.1.1 Darstellung	145
V.2.1.2 Bewertung	146
V.2.2 Elektronische Post	146
V.2.2.1 Darstellung	146
V.2.2.2 Bewertung	147
V.2.3 Verzeichnisdienst	148
V.2.3.1 Darstellung	148
V.2.3.2 Bewertung	148
V.2.4 Sicherheitsmechanismen und Sicherheitsdienste	149
V.2.4.1 Darstellung	149
V.2.4.2 Bewertung	150
V.2.5 Die grafische Benutzeroberfläche	150
V.2.5.1 Darstellung	150
V.2.5.2 Bewertung	152
VI Zusammenfassung und Ausblick.....	154
Anhang.....	156
A Abkürzungsverzeichnis	156
B Literatur	158