
Inhaltsverzeichnis

1	Einleitung	1
1.1	Problemstellung	3
1.2	Aufbau der Arbeit	6
2	Grundlagen	9
2.1	Kommunikationsprotokolle	9
2.2	Schutzziele und Angreifer	13
2.3	Verfahren für Sicherheitsprotokolle	14
2.3.1	Verschlüsselung	14
2.3.2	Signaturen	15
2.3.3	Hashfunktion	16
2.3.4	Message Authentication Codes	16
2.3.4.1	Keyed Hash Message Authentication Code	17
2.3.5	Bereitstellung kryptografischer Schlüssel	18
2.3.5.1	Diffie-Hellman	18
2.3.6	Weitere Verfahren	19
2.3.6.1	Sequenznummern, -zähler und -fenster	19
2.3.6.2	Einmalzahlen	20
2.4	Stärke der Sicherheit	20

2.5	Sicherheitsprotokolle	24
2.5.1	IP Security (IPsec)	24
2.5.2	Transport Layer Security (TLS)	28
2.6	Protokollkomposition	30
2.6.1	Arbeiten zur Protokollkomposition	32
2.7	Entscheidungsverfahren	34
2.7.1	Nutzwertanalyse	34
2.7.1.1	Eigenschaften der Nutzwertanalyse	35
2.7.2	Analytic Hierarchy Process	37
2.7.3	Idealpunktverfahren	38
2.7.4	Outranking-Verfahren	38
2.8	Usability	39
3	Kommunikationseigenschaften	41
3.1	Wahl von Kommunikationsprotokollen	42
3.2	Merkmale von Kommunikationseigenschaften	46
3.3	Kommunikationseigenschaften	47
3.3.1	Dienstgüte	48
3.3.1.1	Latenz und Latenzschwankungen	50
3.3.1.2	Kommunikationsaufbauverzögerung	53
3.3.1.3	Kapazität	56
3.3.1.4	Overhead	57
3.3.2	Zuverlässigkeit	61
3.3.2.1	Verlust	62
3.3.2.2	Duplikate	63
3.3.2.3	Verfälschung	65
3.3.2.4	Reihenfolgetreue	65
3.3.2.5	Übergeordnete Kommunikationseigenschaft	66

3.3.3	Energiebedarf	67
3.3.4	Sicherheit	69
3.3.4.1	Schlüsselaustausch	71
3.3.4.2	Authentifizierung	73
3.3.4.3	Verschlüsselung	74
3.3.4.4	Datenauthenzizität/-integrität	76
3.4	Bestimmung der Kommunikationseigenschaften	76
3.5	Fazit und Zusammenfassung	78
4	Entscheidungsfindung	81
4.1	Anforderungen	81
4.1.1	Eignung der Entscheidungsverfahren	82
4.2	Ablauf der Entscheidungsfindung	84
4.3	Kriterien der Entscheidungsfindung	87
4.4	Nutzenfunktionen	87
4.4.1	Allgemeine Nutzenfunktionen	88
4.4.2	Nutzenfunktionen der Kategorie Dienstgüte	97
4.4.2.1	Internettelefonie	98
4.4.2.2	Videoübertragung	101
4.4.2.3	Terminalanwendung	103
4.4.3	Nutzenfunktionen der Kategorie Zuverlässigkeit	105
4.4.4	Nutzenfunktionen der Kategorie Energiebedarf	107
4.4.5	Nutzenfunktionen der Kategorie Sicherheit	109
4.5	Evaluierung der Entscheidungsfindung	110
4.6	Vergleich mit dem Stand der Forschung	117
4.7	Fazit und Zusammenfassung	120

5	Automatisierte Wahl von Sicherheitsprotokollen	123
5.1	ACCS-Architektur	125
5.2	Sicherheitsmanager	129
5.3	Einflussnahme auf das System	131
5.4	Kommunikationserkenner	134
5.4.1	Erkennen des Aufbaus neuer Kommunikation	135
5.4.2	Ausblick auf weitere Kommunikationserkenner	137
5.5	Anbindung bestehender Sicherheitsprotokolle	138
5.5.1	Schnittstelle zum Anbinden von Sicherheitsadaptern	138
5.5.2	Anbindung des Paketfilters	141
5.5.3	Anbindung von IPsec	141
5.5.4	Anbindung von TLS	145
5.5.5	Automatischer Schutz durch StartTLS	147
5.5.5.1	Evaluierung geschützte E-Mail-Kommunikation	150
5.6	Automatischer Schutz von HTTP	152
5.6.1	Herausforderungen	153
5.6.2	Inhaltsvergleich von HTTP	156
5.6.3	Evaluierung des vorgestellten Verfahrens	158
5.6.3.1	Top-50-Webpräsenzen	159
5.6.3.2	1000 Webpräsenzen	160
5.6.3.3	Parameterwahl	161
5.6.3.4	Gesamtlaufzeit des Webseitenvergleichs	170
5.6.4	Integration in ACCS	174
5.6.4.1	HTTP-Proxy-Ansatz	175
5.6.4.2	Feedback über transparenten Schutz für den Nutzer	177
5.6.4.3	Webbrowser-Erweiterung	181
5.7	Erweiterungen	183
5.7.1	Proaktive Auto-Discovery	184
5.8	Vergleich mit dem Stand der Forschung	185
5.9	Zusammenfassung	186

6	Automatisierte Protokollwahl im zukünftigen Internet	189
6.1	Systemarchitektur für das zukünftige Internet	191
6.2	Aggregation der Wirkungen funktionaler Blöcke	193
6.2.1	Generische Aggregationsformen	195
6.2.2	Latenz	197
6.2.3	Energiebedarf	199
6.2.4	Länge und Overhead	200
6.2.5	Kapazität	201
6.2.6	Zuverlässigkeitseigenschaften	204
6.2.7	Sicherheitseigenschaften	205
6.3	Evaluiierung	206
6.3.1	Ergebnisse	207
6.4	Vergleich mit dem Stand der Forschung	211
6.5	Ausblick: Entwicklungswerkzeuge	214
6.6	Zusammenfassung und Fazit	215
7	Zusammenfassung und Ausblick	217
7.1	Ergebnisse dieser Arbeit	218
7.2	Ausblick und weiterführende Arbeiten	220
A	Kommunikationseigenschaften	221
B	Aggregation der Kommunikationseigenschaften	225
C	Daten der Evaluation der Entscheidungsfindung	229
D	Messergebnisse	233
D.1	HTTP/HTTPS bei den Top-50-Webseiten (DE)	233
D.2	Schützbarkeit von E-Mail-Kommunikation	235
E	Schnittstellenbeschreibung der Sicherheitsadapter	239

F Abkürzungsverzeichnis	241
Literatur	245