

# Inhaltsverzeichnis

<b>1</b>	<b>Einführung</b>	<b>1</b>
1.1	Problemstellung . . . . .	1
1.2	Forschungsfragen . . . . .	3
1.3	Methodische Vorgehensweise . . . . .	5
1.4	Forschungsbeiträge der Dissertation . . . . .	6
1.5	Aufbau der Dissertation . . . . .	8
<b>2</b>	<b>Grundlagen des DNS</b>	<b>11</b>
2.1	Einordnung und Überblick . . . . .	12
2.2	Entwicklung und Entwurfsziele . . . . .	13
2.3	Organisation des Namensraums . . . . .	15
2.4	Architektur des verteilten Systems . . . . .	17
2.5	Resource-Records . . . . .	25
2.6	Verwendete Protokolle . . . . .	28
2.7	Caching . . . . .	41
2.8	Veränderungen seit der Standardisierung . . . . .	52
2.9	DNS-Anwendungen . . . . .	75
2.10	Fazit . . . . .	99
<b>3</b>	<b>Bedrohungen und Sicherheitsmechanismen</b>	<b>101</b>
3.1	Kommunikationsmodell . . . . .	102
3.2	Charakterisierung der relevanten Bedrohungen . . . . .	103
3.3	Ursachen für Bedrohungen . . . . .	104
3.4	Existierende Arbeiten . . . . .	107
3.5	Bedrohung der Verfügbarkeit . . . . .	109
3.6	Bedrohung der Integrität . . . . .	114
3.7	Bedrohung der Vertraulichkeit . . . . .	123
3.8	Fazit . . . . .	134
<b>4</b>	<b>Beobachtung durch rekursive Nameserver</b>	<b>137</b>
4.1	Chancen und Risiken . . . . .	138
4.2	Rekonstruktion des Web-Nutzungsverhaltens . . . . .	142
4.3	Identifizierung der vom Nutzer verwendeten Software . . . . .	187
4.4	Erweiterungsmöglichkeiten und offene Fragen . . . . .	220
4.5	Fazit . . . . .	222

<b>5</b>	<b>Techniken zum Schutz vor Beobachtung</b>	<b>225</b>
5.1	Verzicht auf rekursive Nameserver . . . . .	226
5.2	Anwendbare Datenschutztechniken . . . . .	228
5.3	Analyse des Range-Query-Verfahrens nach Zhao et al. . . . .	237
5.4	DNSMIX-Anonymitätsdienst . . . . .	261
5.5	Erweiterungsmöglichkeiten und offene Fragen . . . . .	289
5.6	Fazit . . . . .	290
<b>6</b>	<b>Verhaltensbasierte Verkettung von Sitzungen</b>	<b>293</b>
6.1	Systematisierung existierender Verkettungsverfahren . . . . .	294
6.2	Konstruktion des verhaltensbasierten Verkettungsverfahrens . . . . .	308
6.3	Empirische Evaluation des Verkettungsverfahrens . . . . .	333
6.4	Einordnung der Ergebnisse . . . . .	397
6.5	Erweiterungsmöglichkeiten und offene Fragen . . . . .	405
6.6	Fazit . . . . .	406
<b>7</b>	<b>Techniken zum Schutz vor Verkettung</b>	<b>409</b>
7.1	Verwendung des Range-Query-Verfahrens . . . . .	410
7.2	Verkürzung der Sitzungsdauer . . . . .	416
7.3	Längere Zwischenspeicherung der DNS-Antworten . . . . .	420
7.4	Erweiterungsmöglichkeiten und offene Fragen . . . . .	427
7.5	Fazit . . . . .	430
<b>8</b>	<b>Schlussfolgerungen</b>	<b>433</b>
8.1	Erkenntnisse und Schlussfolgerungen . . . . .	433
8.2	Einordnung und Anwendbarkeit der Forschungsbeiträge . . . . .	436
8.3	Handlungsempfehlungen . . . . .	439
8.4	Rückblende und Ausblick . . . . .	441
	<b>Literaturverzeichnis</b>	<b>443</b>