

Über Sicherheit und Anonymität in Multicastumgebungen

Dissertation
zur Erlangung des akademischen Grades
DOKTOR-INGENIEUR

des Fachbereichs
Elektrotechnik und Informationstechnik
der FernUniversität – Gesamthochschule
in Hagen

von
Dipl.-Inform. Christian Grosch
Hattingen

Hagen 2001

Antrag auf Zulassung: 2001-07-03
Mündliche Prüfung: 2001-11-09
1. Berichterstatter: Prof. Dr.-Ing. Firoz Kaderali
2. Berichterstatter: Prof. Dr.-Ing. Bernd Krämer

Berichte aus der Kommunikationstechnik
herausgegeben von Prof. Firoz Kaderali

Band 9

Christian Grosch

**Über Sicherheit und Anonymität
in Multicastumgebungen**

Shaker Verlag
Aachen 2002

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Grosch, Christian:

Über Sicherheit und Anonymität in Multicastumgebungen/

Christian Grosch. Aachen: Shaker, 2002

(Berichte aus der Kommunikationstechnik herausgegeben

von Prof. Firoz Kaderali ; Bd. 9)

Zugl.: Hagen, Univ., Diss., 2001

ISBN 3-8265-9814-8

Copyright Shaker Verlag 2002

Alle Rechte, auch das des auszugsweisen Nachdruckes, der auszugsweisen oder vollständigen Wiedergabe, der Speicherung in Datenverarbeitungsanlagen und der Übersetzung, vorbehalten.

Printed in Germany.

ISBN 3-8265-9814-8

ISSN 1437-7497

Shaker Verlag GmbH • Postfach 1290 • 52013 Aachen

Telefon: 02407 / 95 96 - 0 • Telefax: 02407 / 95 96 - 9

Internet: www.shaker.de • eMail: info@shaker.de

Danksagung

Die vorliegende Arbeit entstand während meiner Tätigkeit als wissenschaftlicher Angestellter am Lehrgebiet Kommunikationssysteme des Fachbereichs Elektrotechnik und Informationstechnik der FernUniversität Hagen.

Mein besonderer Dank gilt Herrn Prof. Dr.-Ing. Firoz Kaderali. Durch seine Unterstützung bei der Erstellung der Arbeit, die Diskussionen und wertvollen Hinweise hat er diese Promotion überhaupt erst ermöglicht. Herrn Prof. Dr.-Ing. Bernd Krämer danke ich für das Interesse an der Arbeit und die Übernahme des Korreferats.

Den Mitarbeitern des Lehrgebiets Kommunikationssysteme danke ich sowohl für die interessanten Diskussionen, wertvollen Hinweise und Anregungen zu inhaltlichen Aspekten der Arbeit als auch für ihre individuellen Beiträge zu einem ausgesprochen angenehmen Arbeitsumfeld. Ich habe die vergangenen Jahre stets sehr gern mit ihnen zusammengearbeitet.

Schließlich gilt mein besonderer Dank meiner Frau, meiner Familie und allen, die durch ihre Unterstützung unterschiedlichster Art die Arbeit mit vorangebracht und zu ihrem Gelingen beigetragen haben.

Hattingen im Dezember 2001

Für Petra

Inhaltsverzeichnis

| | |
|--|-----------|
| Abbildungsverzeichnis | xv |
| Tabellenverzeichnis | xviii |
| 1 Einführung und Gliederungsübersicht | 1 |
| 2 Multicastgrundlagen | 5 |
| 2.1 Kommunikationsformen | 5 |
| 2.2 Konzeption | 6 |
| 2.3 Internet Group Management Protocol | 10 |
| 2.4 Protokollvarianten | 12 |
| 2.4.1 Intradomain Routing | 12 |
| 2.4.2 Interdomain Routing | 15 |
| 2.5 MBone | 15 |
| 2.6 Aktuelle Themen | 17 |
| 3 Sicherheit in Multicastnetzen | 19 |
| 3.1 IP-Sicherheit | 20 |
| 3.2 Sichere Gruppenkommunikation | 22 |
| 3.3 Gruppenbezogenes Schlüsselmanagement | 24 |
| 3.4 Offene Fragestellungen | 26 |
| 4 Anonymität in Multicastumgebungen | 29 |
| 4.1 Motivation | 29 |
| 4.2 Zweiseitige Anonymität | 32 |
| 4.3 Mehrseitige Anonymität | 36 |
| 4.4 Problemstellung | 38 |
| 4.4.1 Identität | 39 |

| | | |
|----------|--|-----------|
| 4.4.2 | Kontext und Sicherheitsumgebung | 41 |
| 4.4.3 | Ziele | 48 |
| 4.4.4 | Anforderungen | 48 |
| 4.5 | Zusammenfassung | 49 |
| 5 | Multicast-Anonymisierer | 51 |
| 5.1 | Modellkonzept | 51 |
| 5.2 | Empfängeranonymität | 53 |
| 5.2.1 | Ausgangssituation | 53 |
| 5.2.2 | Unterdrückung von Teilnahmemeldungen | 53 |
| 5.2.3 | Dedicated Multicast Anonymizer | 55 |
| 5.2.4 | Shared Multicast Anonymiser | 62 |
| 5.3 | Senderanonymität | 65 |
| 5.3.1 | Shared Sender Anonymiser | 65 |
| 5.4 | Zugriffskontrolle | 68 |
| 5.4.1 | Grundlegende Konzeption | 68 |
| 5.4.2 | Protokollablauf | 70 |
| 5.4.3 | Anonymer Sender | 72 |
| 5.5 | Serververbund | 73 |
| 5.5.1 | Lastverteilung und Optimierung | 73 |
| 5.5.2 | Mix-Sequenz | 76 |
| 5.5.3 | Erweiterungsmöglichkeiten | 77 |
| 5.6 | Gesamtmodell | 78 |
| 5.7 | Zusammenfassung | 83 |
| 6 | Systembewertung und -optimierung | 85 |
| 6.1 | Kosten von Sicherheitsmaßnahmen | 85 |
| 6.2 | Kosten der Multicast-Anonymisierung | 86 |
| 6.2.1 | Rechenaufwand | 87 |
| 6.2.2 | Speicherbedarf | 90 |
| 6.2.3 | Paketlaufzeiten | 91 |
| 6.2.4 | Netzlast | 91 |
| 6.3 | Paketlaufzeitbetrachtung | 93 |
| 6.4 | Netzlastbetrachtung | 97 |
| 6.4.1 | Grundlegende Fragestellung | 100 |

| | | |
|----------|---|------------|
| 6.4.2 | Verwandte graphentheoretische Problemstellungen | 101 |
| 6.4.3 | Spezifisches Lösungsverfahren | 104 |
| 6.5 | Topologievergleich | 112 |
| 6.5.1 | Netz des DFN, Stand 1999 | 112 |
| 6.5.2 | Netz des DFN, Stand Juni 2000 | 116 |
| 6.5.3 | UUNET-USA | 118 |
| 6.5.4 | CW-USA | 120 |
| 6.5.5 | 8×8-Meshed | 122 |
| 6.5.6 | Vergleich | 125 |
| 6.6 | Zusammenfassung | 126 |
| 7 | Demonstrator | 131 |
| 7.1 | Konzeption | 131 |
| 7.2 | Java-Plattform | 132 |
| 7.3 | Funktionalitäten und Realisierung | 134 |
| 7.4 | Messungen | 136 |
| 7.5 | Zusammenfassung | 140 |
| 8 | Zusammenfassung und Ausblick | 141 |
| A | Abkürzungen | 145 |
| B | Bezeichner- und Funktionsübersicht | 147 |
| C | IP-Adressen Klasse D | 149 |
| D | Sicherheitsstufenkonzept | 151 |
| E | Linkbewertungsalgorithmus | 153 |
| F | Topologien | 157 |
| F.1 | DFN, Stand 1999 | 158 |
| F.2 | DFN, Stand 2000 | 164 |
| F.3 | UUNET USA | 171 |
| F.4 | Cable & Wireless USA | 178 |
| F.5 | Meshed-8×8 | 182 |
| | Literaturverzeichnis | 203 |