

**Stefan Albrecht**

# Unsicherheit in lokalen Netzen

**Diplomarbeit**

## **Bibliografische Information der Deutschen Nationalbibliothek:**

Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de/> abrufbar.

Dieses Werk sowie alle darin enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsschutz zugelassen ist, bedarf der vorherigen Zustimmung des Verlanges. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen, Auswertungen durch Datenbanken und für die Einspeicherung und Verarbeitung in elektronische Systeme. Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Copyright © 1996 Diplom.de  
ISBN: 9783832452711

**Stefan Albrecht**

## **Unsicherheit in lokalen Netzen**

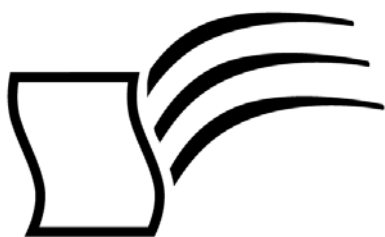


---

Stefan Albrecht

# Unsicherheit in lokalen Netzen

Diplomarbeit  
an der Technischen Universität Dresden  
Fachbereich Informatik  
November 1996 Abgabe



***Diplom.de***

Diplomica GmbH \_\_\_\_\_  
Hermannstal 119k \_\_\_\_\_  
22119 Hamburg \_\_\_\_\_

Fon: 040 / 655 99 20 \_\_\_\_\_  
Fax: 040 / 655 99 222 \_\_\_\_\_

agentur@diplom.de \_\_\_\_\_  
www.diplom.de \_\_\_\_\_

ID 5271

Albrecht, Stefan: Unsicherheit in lokalen Netzen / Stefan Albrecht - Hamburg: Diplomica GmbH, 2002

Zugl.: Dresden, Technische Universität, Diplom, 1996

---

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtes.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Die Informationen in diesem Werk wurden mit Sorgfalt erarbeitet. Dennoch können Fehler nicht vollständig ausgeschlossen werden, und die Diplomarbeiten Agentur, die Autoren oder Übersetzer übernehmen keine juristische Verantwortung oder irgendeine Haftung für evtl. verbliebene fehlerhafte Angaben und deren Folgen.

Diplomica GmbH  
<http://www.diplom.de>, Hamburg 2002  
Printed in Germany

# Inhaltsverzeichnis

<b>1</b>	<b>Einführung - Unsicherheit in Datennetzen</b>	<b>1</b>
<b>2</b>	<b>Klassifizierung von Unsicherheit und Angriffen</b>	<b>3</b>
2.1	ISO-Sicherheitsarchitektur 7498-2 . . . . .	4
2.2	DoD-”Orange Book” und ”Red Book” . . . . .	5
2.3	Systematisierung aus heutiger Sicht . . . . .	7
<b>3</b>	<b>Abhängigkeit von verwendeter Übertragungstechnik und Topologie des Netzwerkes</b>	<b>11</b>
3.1	Broadcastorientierte Netze . . . . .	11
3.1.1	Ethernet . . . . .	12
3.1.2	Token-Ring und Token-Bus . . . . .	12
3.1.3	Fibre Distributed Data Interface . . . . .	13
3.2	Nicht-Broadcastorientierte Netze . . . . .	13
3.2.1	Asynchroner Transfer Modus . . . . .	13
3.3	Zusammenfassung . . . . .	14
3.4	Netzsegmentierung durch Verwendung von Repeatern, Bridges, Routern und Switches . . . . .	15
<b>4</b>	<b>TCP/IP als verbreiteter Protokollstack im LAN und WAN</b>	<b>17</b>
4.1	Überblick über die Bestandteile und das Zusammenwirken im Protokollstack . . . . .	18
4.2	Warum TCP/IP als Demonstrationsgrundlage verwendet wird . .	19
<b>5</b>	<b>Angriffsmöglichkeiten in den einzelnen Protokollschichten und Diensten</b>	<b>21</b>
5.1	Physical Layer/Media Access/Data Link Layer . . . . .	21
5.1.1	Adress Resolution und Reverse Adress Resolution (ARP/-RARP) . . . . .	21
5.2	IP/ICMP Layer . . . . .	22
5.3	TCP/UDP Layer . . . . .	26
5.3.1	RPC-Anwendungen: NFS/NIS . . . . .	30
5.4	Application Layer . . . . .	30
5.4.1	BOOT-Protokoll, File Transfer (TFTP/FTP) . . . . .	30
5.4.2	Mailsystem (SMTP/POP3) . . . . .	31
5.4.3	Remote Login (telnet) . . . . .	32
5.4.4	R-Dienste von BSD-UNIX . . . . .	32

5.4.5	Weitere Dienste und Anwendungen . . . . .	32
5.5	Relevanz und Unterschiede zwischen LAN und WAN . . . . .	34
<b>6</b>	<b>Praktische Angriffsszenarien in einer TCP/IP-Umgebung</b>	<b>37</b>
6.1	Demonstrationen in einer LINUX-Umgebung: Einschränkungen, Grenzen und Möglichkeiten . . . . .	37
6.2	Accountdatensammlung durch Packetsniffing am Beispiel der Dien- ste Telnet und FTP . . . . .	38
6.3	Aktive Beeinflussung des Protokollverhaltens . . . . .	39
6.3.1	IP-Adressmaskerade (IP-Spoofing) . . . . .	41
6.3.2	Angriffe durch gefälschte ICMP-Pakete . . . . .	41
6.3.3	Blockierung der Netzstation durch Datenüberflutung (Brute- Force-/Denial-of-Service-Attack) . . . . .	43
6.3.4	Desynchronisation einer TCP-Verbindung . . . . .	47
6.4	Ausnutzung unsicherer Dienste am Beispiel NIS (Yellow Pages) .	49
6.5	Fälschung von Electronic-Mail-Absenderkennungen . . . . .	51
6.5.1	Mailbomben . . . . .	52
6.6	Zusammenfassung . . . . .	52
<b>7</b>	<b>Systematisierung des notwendigen Aufwands für Angriffe</b>	<b>53</b>
7.1	Informationsbeschaffung und Quellenabschöpfung . . . . .	53
7.1.1	Aktualität der Information . . . . .	54
7.1.2	Einblick in Dienst- und Protokollspezifikationen . . . . .	54
7.2	Zugriff auf Netzstationen mit Systemverwalterrechten . . . . .	54
7.3	Verwendung bestehender Software und Tools . . . . .	55
7.4	Ausnutzung von gewonnenen Erfahrungen und Softwarewied er- verwendung . . . . .	55
<b>8</b>	<b>Gegenmaßnahmen und ihre praktische Umsetzung in der Pro- tokollumgebung</b>	<b>57</b>
8.1	Angriffserkennung und Protokollierung von Aktionen . . . . .	57
8.2	Firewalls und sichere Gateways . . . . .	58
8.3	Verschlüsselung und Datenintegritätssicherung . . . . .	58
8.4	Ausgewählte Schutzmaßnahmen auf Netzwerk-Ebene . . . . .	58
8.4.1	Sicherheitsarchitektur für IP nach RFC1825 . . . . .	58
8.4.2	Verschlüsselung von TCP/UDP durch das swIPe-Protokoll	60
8.5	Testen der Sicherheit durch eigene Systemeintruchs-Versuche . .	61
8.6	Kombination der Einzelmaßnahmen zu einem lückenlosen Sich- erheitsgesamtkonzept . . . . .	61
8.7	Grenzen und Zweckbegrenzung von Maßnahmen . . . . .	61
8.8	Auswirkungen von Datenschutzmaßnahmen auf die Protokoll- performance . . . . .	62
<b>9</b>	<b>Zusammenfassung</b>	<b>63</b>
9.1	Ausblick und offene Probleme . . . . .	64
9.2	Neuerungen durch IPv6 und neue Dienste . . . . .	65



<i>Inhaltsverzeichnis</i>	iii
<b>A Glossar und Abkürzungsverzeichnis</b>	<b>67</b>
<b>B Quellcode der vorgestellten Beispiele</b>	<b>71</b>
B.1 Lizenzbestimmungen verwendeter Software . . . . .	77
<b>C Selbständigkeitserklärung</b>	<b>83</b>

# Abbildungsverzeichnis

2.1	ISO 7498-2 Umsetzung der Sicherheitsfunktionen im Schichtenmodell . . . . .	5
4.1	Zusammenhänge und Zusammenwirken der Komponenten im TCP/IP-Protokollstack . . . . .	18
5.1	Protokollkopf des Internet-Protokolls und IP-Spoofing . . . . .	23
5.2	Datenzugriff über Source-Routing . . . . .	25
5.3	TCP "Three-Way-Handshake" . . . . .	28
6.1	Testumgebung für praktische Angriffsszenarien . . . . .	37
6.2	Verdeutlichung der Paketzusammenstellung über RAW_SOCKET's	40
6.3	Zusammenhang von TCP-Applikation und Socket-Connection-Queue . . . . .	44
6.4	NIS-Spoofing nach [HESS] . . . . .	49
6.5	Austausch der NIS-Nachrichten zwischen Client, Angreifer und Server . . . . .	50
8.1	IP Sicherheitsarchitektur . . . . .	59

# Tabellenverzeichnis

2.1	Aktive Angriffstechniken . . . . .	4
2.2	Unsicherheitsmerkmale nach NCSC-TG-005 Teil II . . . . .	7
2.3	Klassifizierung nach DoD 5200.28-STD . . . . .	9
3.1	Unsicherheit in Physical-/Data-Link-Layer Protokollen . . . . .	14
3.2	Netzsegmentierung im Überblick . . . . .	15
5.1	Angriffe auf IP/ICMP-Ebene . . . . .	23
5.2	Sicherheitsrelevante IP-Optionen . . . . .	24
5.3	Dienste in LAN und WAN . . . . .	35
6.1	Implementierte ICMP-Nachrichten . . . . .	42
6.2	Übertragungseinschränkung durch Datenflutung . . . . .	43
8.1	Processing-Overhead-Messungen im swIPe-Protokoll . . . . .	62
9.1	Angriffe - Aufwand, Schaden und mögliche Gegenmaßnahmen . . .	63