FACTA UNIVERSITATIS (NIŠ)
Series: Electronics and Energetics vol. 12, No. 3 (1999), 47-55

681.3.004.14

RECHNERORIENTIERTE DATENAUFNAHME UND DESSEN VERTEILUNG ZUR ANALYSE

Thomas Droste

Kurzfassung. Der Netzwerkverkehr ist für eine Kollisions Domäne an jedem Rechner mitprotokollierbar, daraus ergibt sich die Möglichkeit, diesen theoretisch an jedem Rechner zur Auswertung heranzuziehen. Ziel dieses Artikels ist es, den Ablauf von der Aufnahme der Daten selbst bis hin zur Verarbeitung darzulegen und auf kritische Punkte hinzuweisen.

1. Einführung

Ein gesichertes Netzwerk verfügt mindestens über eine Firewall, die den Datenverkehr zwischen internem und externem Netz aktiv restriktiert. Dabei terminiert der Datenfluß beidseitig an der Firewall, d.h. ohne Prüfung gelangen keine Daten in das eigene LAN hinein, respektive hinaus. Eine Steigerung der Sicherheit kann durch interne Mechanismen erzielt werden, die hinter einer Firewall im eigenen LAN aktiv arbeiten und den lokale Datenfluß überprüfen. Intern kommen Intrusion Detection Systeme zum Einsatz, die an Koppelpunkten zwischen einzelnen Netzwerkabschnitten eingesetzt werden und den passierenden Netzwerkverkehr überwachen.

Die Möglichkeiten der Sicherung sind damit noch nicht voll ausgeschöpft, da Rechnersysteme theoretisch untereinander unprotokolliert kommunizieren können, ohne daß ein Intrusion Detection System anschlägt, wenn es nicht direkt am Kommunikationsweg konnektiert ist. Erhält ein jeder Rechner einen Mechanismus zur Prüfung des Datenflusses, so kann demnach jede Kommunikation und jeder Datenfluß über das Netzwerk detektiert und geprüft werden. Losgelöst von einem komplexen Netzwerk ist die Betrachtung für einen rechnersensitiven Sicherheitsmechanismus unter

Manuscript eingegangen Aug. 22, 1999.

Dipl.-Ing. Thomas Droste, Wissenschaftlicher Mitarbeiter, Lehrstuhl für Datenverarbeitung, Ruhr-Universität Bochum, 44780 Bochum, E-mail: droste@etdv.ruhr-uni-bochum.de .

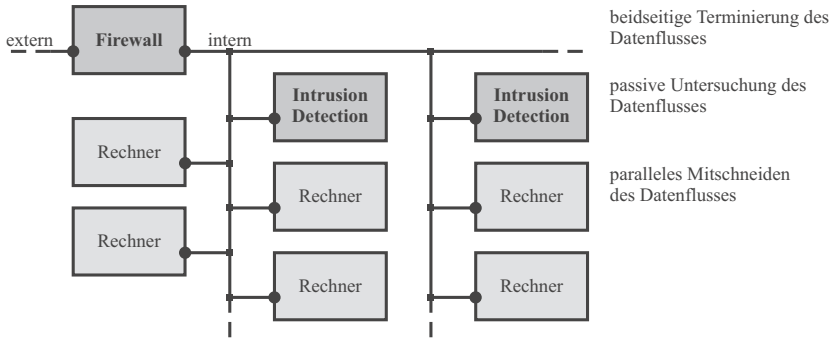

Abb. 1. Anordnung der Sicherheitskomponenten in einem LAN

zwei Aspekten zu sehen: zum einen die Erfassung der Daten selbst und zum anderen die Weiterverarbeitung lokal oder im Netz verteilt.

Abbildung 1 verdeutlicht die Kombination der obigen Konzepte. Der Datenfluß terminiert an der Firewall, d.h. jedes Datenpaket muß durch die Firewall und dessen Sicherheitsüberprüfung. Eine Intrusion Detection ist an Koppelpunkten angeordnet, die bereits hinter einem durch eine Firewall gesicherten Bereich liegen. Hier findet ein passive Untersuchung des Datenflusses statt, d.h. jedes Paket wird untersucht, aber der Datenfluß wird nicht unterbrochen bzw. beeinflußt. Die einzelnen Rechner besitzen jeweils einen integrierten Sicherheitsmechanismus. Als aktiver Kommunikationspartner nehmen sie als normaler Endpunkt an einer Kommunikation teil, unabhängig von der zusätzlich stattfindenden parallelen Datenaufnahme. Sie schneiden den Datenfluß parallel mit, auch wenn sie nicht Endpunkt einer Verbindung sind.

2. Datenaufnahme

Die Datenaufnahme an einem einzelnen Rechner erfolgt parallel zum normalen Netzwerkverkehr. D.h. die Kommunikation zwischen diesem Rechner und einem andern Kommunikationspartner wird nicht beeinflußt. Folglich bleibt die Datenübertragungsrate für die rechnerspezifische Kommunikation maximal. Andernfalls, wenn ein wie in einer Firewall implementierter Filtermechanismus eingesetzt wird, hängt die Übertragungsrate von der Geschwindigkeit des Rechners bzw. des Filters und dessen Prüfalgorithmus ab. Übertragene Daten in Netzen bestehen aus einem Kommunikations- und Nutzdatenanteil, also aus dem Header respektive den eigentlichen Daten.

Eine Differenzierung des Datenflusses erfolgt daher in zwei Schritten:

paketflußorientiert und dateninhaltsspezifisch.

Der Kommunikationsanteil ist für die Flußkontrolle von Bedeutung, da nicht nur einzelne Pakete, sondern ein Kommunikationsverlauf charakterisiert werden kann. Die einzelnen Header eines jeden Paketes sind für die Auswertung wichtig, da bereits ein einzelnes Paket eine Sicherheitsverletzung, bzw. den Anfang eines möglichen Angriffs mit sich ziehen kann. Ein Ping-Befehl z.B. offenbart dem Sender sofort die Information über Erreichbarkeit und Existenz eines Systems. Ebenso kann eine angeforderte Telnet-Sitzung bereits durch das erste Paket erkannt werden, da eine charakteristische Kommunikation stattfindet. Neben den unerlaubten Zugriffen, die im Prinzip durch die vorgestellten Sicherheitseinrichtungen abgeblockt werden, ist die normale Kommunikation innerhalb des LAN im Verhältnis dazu um ein vielfaches höher. Status- und Broadcast-Meldungen zwischen Rechnern, Switches, Routern etc. stellen in Netzwerken eine Grundlast dar. Hinzu kommen die gezielten Verbindungen der lokalen Benutzer, wobei neben DNS-Anfragen die entsprechenden Dienste genutzt werden. Die Aufnahme eines jeden einzelnen Paketes ist somit erforderlich.

Auf der Anwenderebene, z.B. bei der Übertragung von Dateien, ist der Inhalt der Daten selbst zur Auswertung heranzuziehen. Sind die Daten z.B. ausführbare Programme oder Archive, können Viren oder Trojanische Pferde enthalten sein. Durch den Einsatz zentraler Virenscanner wird dieses Sicherheitsproblem erkannt und beseitigt.

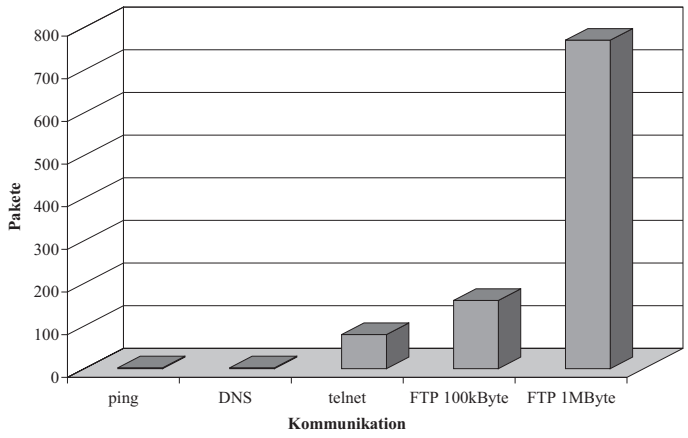

Abb. 2. Anzahl der Pakete für unterschiedliche Kommunikationen

In Abbildung 2 ist die Anzahl der Pakete mehrerer Kommunikationsarten prinzipiell dargestellt, um die Wichtigkeit einzelner Pakete hervorzuheben. Bei einem Ping-Befehl an ein Zielsystem werden zwei Pakete (ICMP-Echo-Request, ICMP-Echo-Reply) übertragen. Eine DNS-Anfrage benötigt ebenfalls zwei Pakete. Eine Telnet-Sitzung über den Dienst erfordert mehrere Pakete. Dabei ist in obigem Beispiel nur eine Verbindung aufgebaut, der Benutzer mit Kennwort angemeldet und anschließend die Sitzung beendet worden. Durch weitere Aktionen, wie z.B. Ausführen von Befehlen und Ausgaben auf der Konsole, erhöht sich die Paketzahl. Da der Benutzer auf dem entfernten Zielsystem arbeitet, werden nur Informationen zur Ausgabe weitergegeben. Die Kommunikation läuft langsam ab. Es handelt sich nicht um einen kontinuierlichen Datenfluß, in dem die Befehle und Ausgaben übertragen werden. Bei einer FTP-Sitzung läuft die Kommunikation zum Aufbau und zur Ausführung der Befehle, analog zu einer Telnet-Sitzung, auch zeitgedehnt ab. Erst bei einer Übertragung einer Datei wird ein anhaltender Datenstrom übermittelt, der im Gegensatz zur normalen Kommunikationsaufkommen einer FTP-Sitzung um ein vielfaches höher ist. Das Verhältnis von benötigten Pakete für das Initiieren einer Verbindung und der Übertragung einer Datei von 100 kByte ist noch in etwa gleich, dagegen überwiegt der Dateiübertragungsanteil bei einer Dateigröße von z.B. 1 MByte. Dieser Datenstrom ist auffälliger, da er eine Kontinuität aufweist, welche für Einzelpakete nicht vorhanden ist. Somit wird deutlich, daß eine Kommunikation frühstmöglich klassifiziert werden muß. Einen Schritt vor einer angeforderten Verbindung steht die Erreichbarkeit des Zielrechner bzw. des Dienstes selbst. In diesem Fall werden im Höchstfall einzelne Pakete Übertragen, da das Zielsystem nicht konnektiert werden kann bzw. der Dienst nicht verfügbar ist.

Eine Datenaufnahme ist nur unter der wesentlichen Voraussetzung, daß die Rechte für diesen Eingriff auf die untersten Ebenen und damit auf den Pakettreiber der Netzwerkkarte bestehen, möglich. Diese Voraussetzung ist dabei von zwei unterschiedlichen Seiten der Sicherheit zu betrachten. Einerseits können Daten nur aufgenommen werden, wenn ein Systemadministrator oder gleichberechtigter Systembetreuer die Rechte für einen Rechner besitzt. Andererseits ist ein Rechner, der nicht dem Systembetreuer unterliegt, ein mögliches Sicherheitsrisiko. Eine Aufnahme der Daten kann bei letzterem auch ohne Kenntnis des Systembetreuers erfolgen, da die Rechte zum Zugriff auf die Netzwerkkarte unter Umständen für andere, als lokaler Administrator auf einem Rechner, möglich ist. Die Gefahr wird z.B. bei der Emailabfrage über das POP3 deutlich. Die Paßwörter werden im Klartext über das Netz übertragen und können theoretisch von jedem Rechner, der in der selben

Kollisions Domäne des Rechners bzw. Email-Servers liegt, mitgeschnitten werden. Folglich ist der gesamte dortige Netzwerkverkehr unsicher und kann aufgenommen und beliebig ausgewertet werden. Gegenmaßnahmen liegen in einer restriktiven Sicherheitspolitik, welche keine administrativen Rechte auf Rechner für lokale Benutzer zuläßt, oder in einer Ausgliederung kritischer Systeme. Eine weitere Maßnahme ist der Einsatz von Verschlüsselungen, damit der Datenverkehr schwer auswertbar wird.

Wenn alle Voraussetzungen zur Datenaufnahme bereit stehen und eine entsprechende Sicherheitspolitik besteht, kann die Auswertung der Daten erfolgen, damit Sicherheitsrisiken minimiert werden und auch z.B. der obige Fall erkannt wird.

3. Verarbeitung

Die Datenmenge, die durch die Datenaufnahme erreicht wird, muß entsprechend verarbeitet, also ausge- bzw. bewertet werden. Es stellt sich die Problematik zwischen lokaler contra globaler Auswertung. In Abhängigkeit der aufgenommenen Daten ist es sinnvoll, eine Kombination beider Weiterverarbeitungsstrategien zu nutzen.

Die lokale Auswertung ist für einfache Regelsätze bezüglich des Rechners, die zudem quasi in Echtzeit ausführbar sind, sinnvoll. Dabei werden die Datenpakete per Filteroptionen verglichen, analog zu einer klassischen Firewall. Der Nachteil besteht in der fehlenden Interaktion mit anderen Systemen, da die Auswertung nur bezüglich des Rechners bzw. des lokalen Regelsatzes durchgeführt wird.

Bei einer verteilten Auswertung werden die Daten nur einmal je System aufgenommen. D.h. die zur lokalen Auswertung genutzten Daten werden für die Verteilung ebenfalls benutzt. Die beteiligten Systeme kombinieren ihren Datenbestand, wodurch der systemübergreifende Datenstrom analog zur lokalen Auswertung überprüft werden kann. Zusätzlich ist es möglich, Langzeitauswertungen durchzuführen, indem z.B. eine Angriffsmustererkennung über einige bzw. alle Systeme eine Sicherheitsverletzung aufdeckt. Im Gegensatz zur sofortigen lokalen Datenanalyse bleiben bei einer Langzeitanalyse die aufgenommenen Daten zunächst verfügbar. Dadurch ist eine zeitversetzte Analyse möglich. Ein weiterer Vorteil liegt in der erzielten Redundanz, da die Daten verschiedener Quellen zusammengefügt werden. Es müssen gleiche Daten von mehreren Datenquellen vorliegen, ansonsten liegt eine Manipulation vor.

Durch die Kombination und Interaktion zwischen den Systemen wird der Netzwerkverkehr stark erhöht. Es muß zumindest das doppelte Daten-

volumen übertragen werden, da jedes System seine aufgenommenen Daten zur Weiterverarbeitung an andere Systeme übergibt. Unter der Voraussetzung, daß ein Rechner zum Empfang der Daten von anderen Systemen benutzt wird und n Systemen zur Datenaufnahme beteiligt sind, wird ein in der Kollisions Domäne übertragenes Paket n mal übertragen: das Originalpaket von einem/an ein System und die Übertragung von allen $n-1$ Systemen zur zentralen Datensenke. Die aufgenommenen Daten der zentralen Datensenke werden dabei intern verarbeitet und fallen für die Anzahl der als Kopie übertragenen Daten über das Netz heraus.

Dieses Problem läßt sich durch optimale Nutzung schwacher Netzwerkbelastung ausgleichen. Problematisch ist auch die Bildung der kombinatorischen Filter, die komplexer auf das Netzwerk definiert werden müssen. Neben den Regeln zur Sicherung werden Systeminteraktionen mit in die Prüfung eingearbeitet. Die Angreifbarkeit des zu übermittelnden Datenstromes zur verteilten Auswertung ist ein zusätzlicher Unsicherheitsfaktor, der jedoch leicht durch Verschlüsselung desselben behoben werden kann.

Zusammenfassend ist die Kombination von lokaler und verteilter Auswertung sinnvoll, da die Last für ein Einzelsystem auf mehrere Systeme aufgeteilt und somit die Verfügbarkeit der Einzelsysteme gewährleistet wird. Zum Erreichen dieses Zieles sind jedoch besonders bei der verteilten Analyse weitere Mechanismen einzusetzen, welche eine Entlastung der Einzelrechner auch im verteilten System zuläßt.

4. Realisierbarkeit

Bei der Realisierung stellt sich zunächst eine wichtige Frage: Können wirklich alle Daten aufgenommen werden, die an einem Rechner anliegen? Theoretisch ist es möglich, dies zu erreichen, wenn das System schnell in Bezug auf die Aufnahme ist. Es dürfen somit keine intensiven Rechenprozesse auf dem Rechner laufen, die das System blockieren. Für die Aufnahme wird die Netzwerkkarte in den Promiscuous-Modus gesetzt, wodurch alle an die/von der Netzwerkkarte adressierten bzw. passierenden Daten parallel zum übrigen Datenverkehr, sowohl lokal als auch im übrigen Netzsegment, aufgenommen werden können. Probleme entstehen bei der lokalen Sicherung der Daten, wenn der lokale Rechner stark belastet ist. Findet dann eine Echtzeitprüfung der einzelnen Pakete statt, könne Lücken entstehen, wenn die Filterung nicht vor dem nächsten Eintreffen eines Paketes abgeschlossen ist. Abhilfe schafft eine minimal versetzte Auswertung, damit eine vollständige Aufnahme und eine quasi Echtzeitauswertung stattfinden kann. Zu unterscheiden sind somit zwei Arten der Datenaufnahme: langsame, zeitgedehnte und schnelle, volumenkompakte Daten.

Erstere können z.B. bei Telnet-Sitzungen analysiert werden, da einzelne Pakete relativ langsam zwischen den Zielsystemen übermittelt werden. Eine Echtzeitprüfung ist dadurch einfacher möglich. Die schnellen, volumenkompakten Daten, z.B. bei einem FTP-Download, haben einen höheren Datendurchsatz, aber es ist eine geringerer Aufwand für die Prüfung des Headers notwendig. Der Inhalt der Übertragung, also z.B. eine Datei, ist wichtiger. Erst nach abgeschlossener Übertragung ist eine Prüfung der Gesamtdaten, z.B. auf Viren, sinnvoll. Die Aufnahme kann somit auch parallel gut abgearbeitet werden.

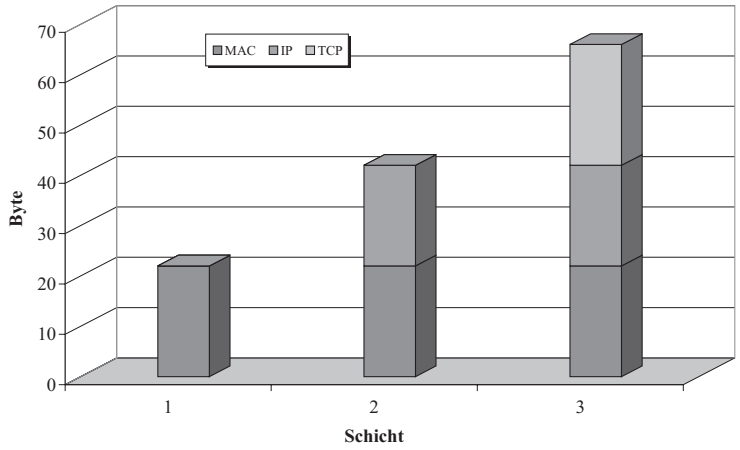

Abb. 4. Minimaler Headeranteil im TCP/IP-Schichtenmodell am Beispiel einer TCP-Verbindung

Das Problem bei der Echtzeitanalyse liegt in der Filterung der Daten. Werden prinzipiell alle Daten aufgenommen, so ist es kein Problem, diese zu sichern. Wird jedoch direkt ein Paket untersucht, so sinkt die Durchsatzrate des Filters. Mit Hilfe eines Softwaretools zur Protokollierung und Analyse des Datenstroms [1] ist die Abhängigkeit deutlich festzustellen. Ausgangspunkt ist die notwendige Untersuchung der Pakete. Der einfachste und unkritischste Fall ist, ein Paket ohne Interpretation, also ohne direkte Filterung, aufzunehmen. In Abbildung 4.1 ist die minimal notwendige Header-Größe auf den verschiedenen Schichten mit ihrer Aufsummierung dargestellt, wobei keine Optionsfelder belegt sind. Die Auswertung der Informationen aus den einzelnen Headern erfolgt gleich. Die relevanten Daten werden durch Filterung aus dem Paket extrahiert und verglichen. Auf der 1.Schicht im

TCP/IP-Schichtenmodell, der Netzzugangsschicht, können somit die MAC-Adressen der Kommunikationspartner ermittelt werden. Auf der 2.Schicht, der Internetschicht, sind z.B. die IP-Adressen extrahierbar. Die Header-Größe beträgt auf dieser Schicht minimal 20 Byte, maximal 60 Byte. Der nachfolgende Header der 3.Schicht, der Transportschicht, ist somit wiederum erst unter Berücksichtigung der vorangestellten Header zu überprüfen. Auf der 3.Schicht kann dann z.B. der Port einer Kommunikation ermittelt werden. Der Zeitaufwand steigt mit jeder Prüfung: zum einen mit der Anzahl der Filterkriterien und zum anderen mit der Komplexität und Abhängigkeit der Filter untereinander. Das Problem bei einer schnellen Analyse liegt in der Variationsbreite der einzelnen Pakete bezüglich des Aufbaus und der gesuchten Merkmale der Filter. Um auf der 3.Schicht z.B. die Filterung nach Port-Nummern durchzuführen, ist eine vorhergehende Prüfung der Header-Teile der unteren Schichten notwendig. Erst dann kann das Filter auf diese Schicht angewendet werden. Weiterhin ist zu beachten, daß auch andere Protokolle übertragen werden können, die wiederum auch erkannt und identifiziert werden müssen. Eine reine Echtzeitanalyse an einem Rechner, der parallel zum normalen Kommunikation die Daten mitschneidet, ist nicht möglich. Es werden jeweils nur einzelne Pakete mitprotokolliert und diese erst ausgewertet bevor ein neues Paket eingelesen wird. Bei einer geringen Netzwerkauslastung bzw. keinem konstantem Datenstrom liefert die Analyse noch alle Pakete. Bei anhaltendem Datenstrom fallen aber Pakete heraus, da die Analyse Zeit benötigt und die nachfolgenden Pakete schneller am Rechner eintreffen, als die Analyse abgeschlossen ist. Eine quasi Echtzeitauswertung durch Zwischenspeicherung löst das Problem der eventuell fehlenden Datenpakete. Die Aufnahme erfolgt dabei immer noch parallel, aber mittels FIFO in einen Puffer. Anschließend kann jedes Paket einzeln ausgewertet werden ohne ein Paket durch mangelnde Verarbeitungsgeschwindigkeit auszulassen.

5. Ausblick

Wie bereits angedeutet, ist unter Verarbeitung durch Verteilung nicht nur die Aufteilung der Daten zu verstehen, sondern vielmehr ein intelligentes, sich selbst anpassendes System, welches automatisch eine Auswertung durchführt. Dabei ist es wichtig, nicht nur eine Auswertungsinstanz einzusetzen und die selben Rechner bestimmte Aufgaben erfüllen zu lassen, sondern diese Aufgaben ebenfalls zu verteilen. Ein weiteres Kriterium ist der Vertrauensgrad eines Rechners. Durch die Kompromittierung eines Rechners oder Netzwerks muß der Datenstrom weiterhin konsistent sein. Eine Verschlüsselung muß dabei obligatorisch eingesetzt werden, da die mitprotokollierten Daten, welche an einen anderen Rechner zur Analyse weitergeleitet

werden wiederum die Originaldaten enthalten. Ein weiterer Vorteil der Verschlüsselung ist die Eindeutigkeit des Absenders der Daten. Da verschiedene Quellen die gleichen Informationen, jedoch verschieden verschlüsselt und jeweils rechnerbezogen übermitteln, ist eine Manipulation im Datenstrom schwieriger, da gleichzeitig alle n Systeme kompromittiert werden müssen.

Dies sind nur einige Punkte, wie sich die rechnerorientierte Datenaufnahme und dessen Verteilung zur Analyse weiterentwickeln läßt. Dabei sind u.a. noch keine konkreten Algorithmen angesprochen worden, um z.B. eine Verteilung durchzuführen oder die verfügbaren Ressourcen eines Rechner optimal auszunutzen.

Dank

Herrn Prof. Dr.-Ing. Wolfgang Weber danke ich für die bisherige und auch weiterführende Unterstützung, durch die es möglich ist das weite Spektrum, welches in diesem Artikel beschriebene wird, zu untersuchen und geeignete Lösungen zu finden.

LITERATUR

1. H. Baumann: *Entwicklung eines Softwaretools zur Protokollierung und Analyse des Datenstroms in Netzwerken.* Diplomarbeit D344, Lehrstuhl für Datenverarbeitung, Ruhr-Universität Bochum, 1999
2. D.B. Chapman, E.D. Zwicky: *Building Internet Firewalls.* O'Reilly & Associates Inc., Sebastopol, 1995
3. T. Droste, W. Weber: Moderne Firewalls für LANs: *Facta Universitatis, Series: Electronic and Energetics.* vol.11, No.3 (1998), pp..
4. A. Paweletz: *Analyse verschiedener Verschlüsselungsverfahren geeigneter Umsetzung in einer Client-/Server-Applikation zum automatisierten Datentausch.* Diplomarbeit D339, Lehrstuhl für Datenverarbeitung, Ruhr-Universität Bochum, 1999
5. W.R. Stevens: *TCP/IP Illustrated.* Vol. 1, Addison-Wesley Publishing Company, Reading, 1994