inforum

INFOrmationsforum des Rechenzentrums der Universität Münster

Jahrgang 21, Nr. 3 – Juli 1997 ISSN 0931-4008

Inhalt

Impressum

infoforum
ISSN 0931-4008

Westfälische Wilhelms-Universität
Universitätsrechenzentrum
Einsteinstr. 60
48149 Münster

E-Mail: urz@uni-muenster.de
WWW: http://www.uni-muenster.de/URZ/

Redaktion: W. Bosse (✆ 83-31561, ✉ bosse@uni-muenster.de)
R. Perske (✆ 83-31582, ✉ perske@uni-muenster.de)
H. Pudlatz (✆ 83-31672, ✉ pudlatz@uni-muenster.de)
E. Sturm (✆ 83-31679, ✉ sturm@uni-muenster.de)

Satzsystem: Corel WordPerfect 7.0 für Windows 95/NT

Druck: Universitätsrechenzentrum
(Rank Xerox DocuTech 135)

Auflage dieser Ausgabe: 1500

Editorial

H. Pudlatz

Diese Ausgabe steht in mehrerlei Hinsicht unter dem Leitgedanken „Computer und Recht“.

Je mehr der Computernutzer nicht mehr mit seinem PC isoliert im stillen Kämmerlein sitzt, sondern mit anderen Computernutzern kommuniziert, desto mehr hat er sich mit gesellschaftlichen Belangen und nicht zuletzt mit Fragen des Rechts auseinanderzusetzen. Vielen Nutzern ist aber wenig oder gar nicht bewußt, welche rechtlichen Probleme z. B. mit der Verbreitung oder auch nur der Nutzung von Text-, Bild- oder Audio-Informationen im Internet verbunden sein können.

Wir möchten unseren Lesern insbesondere einen Beitrag von Dr. jur. Stefan Ernst aus Freiburg (i. Br.) zur Beachtung empfehlen. Herr Dr. Ernst versteht es, unter weitgehender Vermeidung der juristischen Fachsprache die behandelten Probleme auch Nichtjuristen zu verdeutlichen (vgl. auch seinen Artikel „Rechtsfragen für Internet-User“ in infoRUM Nr. 2/1996). Wir danken Herrn Dr. Ernst für die Erlaubnis zum Nachdruck seines Artikels. Zugleich sei darauf hingewiesen, daß an der Universität Münster die kompetente Adresse für Rechtsfragen um Computer und Netze das Institut für Informations-, Telekommunikations- und Medienrecht ist (Prof. Dr. Thomas Hoeren). Hier kann im Ernstfall um Rat nachgefragt werden.

Weitere Gedanken zur Rechtsthematik finden Sie auch im Artikel „Kostenerstattung bei mißbräuchlicher Nutzung der Netze“ und – insbesondere im Hinblick auf elektronische Unterschriften – im Artikel „Kryptografische Fingerabdrücke“. Auch im Artikel „Netzprobleme bei mangelnder Qualität von Anschlußkabeln“ werden rechtliche Überlegungen aus der Sicht eines Netzbetreibers angestellt.

Wenn Sie in der Rubrik RUM-Lehre die Vorlesungsankündigungen für das Wintersemester 1997/98 vermissen, so hat dies seinen Grund darin, daß Lehre im neuen IV-Versorgungskonzept der Universität im Universitätsrechenzentrum (Zentrum für Informationsverarbeitung) auf Grund eines Senatsbeschlusses nicht mehr stattfindet („Lehre ist Angelegenheit der Fachbereiche“). Als *effiziente Form der Beratung* war die Lehre 33 Jahre lang ein zentrales Anliegen des Rechenzentrums. Daß hier ein gleichbleibend hoher Bedarf bestand, belegen die großen Hörerzahlen.

Die Ferienkurse im September waren bereits angekündigt und finden also noch statt. Nutzen Sie diese Gelegenheit! Denn Beratung soll zukünftig verstärkt auf andere Weise erfolgen: „vor Ort“, telefonisch oder per E-Mail.

RUM-Aktuell

Ausbildungsveranstaltungen zu Themen der DV

W. Held

Ab dem kommenden Wintersemester bietet das Universitätsrechenzentrum keine Lehrveranstaltungen mehr an.

Der Senat hat auf Vorschlag des Rektorats beschlossen, daß das IV-Zentrum (Universitätsrechenzentrum) zukünftig keine Kurse mehr zu Themen der DV anbieten soll. Die Lehre ist ausschließlich in die Verantwortung der Fachbereiche gestellt worden.

Wir bitten alle Studierenden, die sich auf unser regelmäßiges Angebot im Wintersemester 1997/98 verlassen haben, um Nachsicht.

Allerdings wird in für den Bereich der Informationsverarbeitung eingerichteten Gremien der Universität derzeit noch über den Bedarf an fächerübergreifenden Ausbildungsveranstaltungen und deren Durchführung beraten.

Netzausbaupläne des MWF

W. Held

Die für die Hochschulen in Nordrhein-Westfalen zuständige Ministerin, Frau Anke Brunn, hat am 2.7.97 in einem Vortrag deutlich gemacht, wie die Landesregierung den Ausbau der Kommunikationsnetze in NRW fördern will.

Der Anschluß der nordrhein-westfälischen Hochschulen an das Wissenschaftsnetz soll in einem überschaubaren Zeitraum von 34 MBit/s über 155 auf 622 MBit/s ausgebaut werden. Auch der Übergang auf Gbit/s-Kapazitäten erscheint in nicht allzu weiter Ferne möglich zu sein. In den Hochschulen sollen die lokalen Netze weiter ausgebaut werden, so daß die Kommunikationsmöglichkeiten dem wachsenden Bedarf entsprechen. Schließlich werden im Rahmen des HSP-III-Förderprogramms massiv multimediale Anwendungen in der Lehre gefördert. Bibliotheken gehen mit großen Schritten zu elektronischen Zeitschriften über.

Die Ministerin hat dazu in Anlehnung an das Internet II die Schaffung eines EuroNet II vorgeschlagen, um mit den Entwicklungen in den USA mitzuhalten und diese möglicherweise noch zu übertreffen. Dazu laufen nach den Worten der Ministerin in NRW neben den HSP-III-Aktivitäten interessante Großprojekte wie

- das Gigabit-Testnetz von Aachen über Jülich und die GMD bis nach Essen,
- der in Vorbereitung befindliche Sprachdienst im B-Win (ein DFN-Projekt, an dem Aachen, Köln, Düsseldorf und Münster jeweils mit den technischen Diensten und den Hochschulrechenzentren beteiligt sind) sowie
- das Projekt Internet-Protokoll IPnG (im Rechenzentrum der Universität Münster).

Weitere Einzelheiten findet man über die URL `http://www.mwf.nrw.de/`.

Stockender LAN-Ausbau in der Universität

W. Held

Fehlende Mittel und personelle Probleme lassen den LAN-Ausbau ins Stocken geraten.

Das Universitätsrechenzentrum ist für den LAN-Ausbau in der Universität zuständig. Es beauftragt dazu u. a. auch einzelne Firmen. Da der flächendeckende Ausbau mit Landesmitteln in diesem Jahr noch stockt (im nächsten Jahr hoffen wir hierfür auf zusätzliche Landesmittel), werden sehr viele kleine und mittlere Ausbauaufträge an uns herangetragen, die aus verschiedenen Mitteln finanziert werden.

Derzeit sind 285 kleine und mittlere Ausbauprojekte nicht abgeschlossen. Einige größere Projekte sollten auf Wunsch des Rektorats noch in Auftrag gegeben werden. Wir bitten um Nachsicht, daß wir dieser Auftragsflut nicht mehr in vernünftigen Zeiträumen nachkommen können, denn kleine und kleinste Projekte machen verglichen mit flächendeckenden großen Projekten überproportional viel Aufwand, und in dieser Situation sind von den Verantwortlichen hochschulintern im Netzbereich Stellen gesperrt worden.

Kostenerstattung bei mißbräuchlicher Nutzung der Netze

W. Held

Mißbräuchliche Nutzung der Netze verursacht oft extrem hohe Kosten zu Lasten der Allgemeinheit.

Einige wenige Personen nutzen die Kommunikationsnetze leider immer wieder mißbräuchlich. Sie bringen dadurch nicht nur die Universitäten und ihre Mitglieder in Mißkredit. Sie verursachen auch Kosten auf Rechnern und in Netzen sowie bei den Mitarbeiterinnen und Mitarbeitern im Universitätsrechenzentrum, die Mißbräuche z. B. im Auftrag des *Computer Emergency Response Team (CERT)* oder der Kriminalpolizei verfolgen und an der Aufklärung mitwirken müssen.

Mißbräuche liegen vor, wenn gegen die Gesetze verstoßen wird (Rechts-/Linksradikale Informationen, Wirtschaftskriminalität, Kinderpornografie usw.). Mißbrauch liegt aber auch schon bei nicht strafbaren Informationsangeboten oder -transfers vor, die nicht in Einklang mit Forschung und Lehre zu bringen sind. Dazu gehört z. B. auch die Verteilung von Massenwerbungen an große Nutzergruppen, die dazu nicht ihre Einwilligung erteilt haben.

Die IV-Kommission (früher ADV-Kommission) hat in ihrer letzten Sitzung beschlossen, daß in allen Mißbrauchsfällen die aufgetretenen Kosten von den Verursachenden zu erstatten sind.

SPSS

S. Zörkendörfer

Im Dezember beginnt für die Hochschul-landeslizenz zum Statistik-Paket SPSS ein neues Lizenzjahr.

Mit der Verbreitung von Windows NT und Windows 95 hat die 7er-Version des SPSS nun auch an unserer Universität seine Anhängerschaft gefunden. Bei der Umrüstung unserer Rechner im CIP-Pool Einsteinstraße auf Windows NT soll diese Version ebenfalls dort Einzug halten und die 6er-Versionen ablösen – bei meiner letzten Lehrveranstaltung zum SPSS konnte ich im SS 97 leider nur die Version 6.1.3 nutzen.

Ich ergreife an dieser Stelle gerne die Gelegenheit, den Kollegen in Bonn und Köln meinen und unseren Dank für ihre Bemühungen bei der Betreuung dieser Lizenz auszusprechen. Durch ihre Initiative und Mitwirkung konnte eine CD-ROM aufbereitet und in entsprechender Auflage bereitgestellt werden, die eine einfachere Verteilung dieser Software auch bei uns ermöglicht. Dies betrifft die Produkte

- SPSSWIN 7.5e für Windows 95 und Windows NT,
- SPSSWIN 6.1.3d und SPSSWIN 6.1.3e für Windows 3.x/95/NT,
- dazu die Zusatzprodukte Amos3.6 und CHAID,
- SPSS/PC+ 5.0.2 für MS-DOS,
- SPSS/Mac 6.1.2e für Macintosh,
- SPSS/Mac 6.1.2e für den PowerMacintosh
- sowie Axum 5.0 für Windows 3.x/95/NT.

Bei Einstieg über die WWW-Seite `http://www.uni-muenster.de/URZ/Organisation/PCSoftwareGesamtliste.html` finden Sie im Internet nähere Angaben zur Weitergabe von SPSS-Produkten.

Zur Vorbereitung auf das folgende Lizenzjahr bitte ich um Meldungen, ob von Instituten oder Fachbereichen eine Erweiterung der SPSS-Landeslizenz um zusätzliche Produkte gewünscht wird und mitfinanziert werden kann. In Diskussion steht eine Einbeziehung von *SPSS Missing Value Analysis for Windows 95/NT* und von *Neural Connection*. Zu einer Beschreibung dieser Produkte verweise ich auf die WWW-Seiten `http://www.spss.com/software/spss/base/mva1.htm` und `http://www.spss.com/software/neuro/`.

Einführung des Distributed File Systems

Unix-Systemgruppe

Die Umstellung auf DCE/DFS sorgt für Änderungen bei den Plattenplatzquoten, bei den Dateizugriffsrechten und bei einzelnen Unix-Befehlen.

Im Rahmen unserer umfassenden Umstellung der Systemverwaltung auf DCE (*Distributed Computing Environment*) haben wir damit begonnen, nach den Systemdaten jetzt auch die Daten unserer Unix-Nutzer, die sogenannten *Home Directories*, in Plattenbereiche zu verschieben, die von der DCE-Komponente DFS (*Distributed File System*) verwaltet werden.

Dabei wird jedem Nutzer ein *Fileset* zugeordnet, in dem alle Dateien abgelegt werden und dessen maximale Größe durch eine sogenannte *Quota* festgelegt wird. Die *Filesets* befinden sich in einem oder mehreren *Aggregates*, welche jeweils als *Local File Stores (LFS)* organisiert ist. Ein *Local File Store* ist ein Plattenbereich auf einem *File Server*. *Filesets* können jederzeit von einem *Aggregate* in ein anderes verschoben werden, selbst auf einen anderen Server, ohne daß der Nutzer es bemerkt.

Die *Quota* eines *Filesets* wird bei neuen Nutzern auf 10 MB festgelegt, erfahrungsgemäß ein für 99 % unserer Nutzer ausreichender Wert. Durch diese Quotierung wird das in den letzten Jahren ständig bestehende Problem gelöst, daß einzelne Nutzer die Plattenbereiche mit ihren Daten füllten und dadurch Tausende von anderen Nutzern am Arbeiten hinderten. Die Größe eines *Aggregates* wird durch den verfügbaren Plattenplatz festgelegt. Der Unix-Befehl `df` liefert im DCE/DFS keine sinnvolle Ausgabe mehr, statt dessen sollten Sie jetzt den Befehl `fts lsquota .` verwenden, der die Auslastungszahlen sowohl des *Filesets* als auch des *Aggregates* anzeigt:

```
Fileset Name   Quota    Used  % Used   Aggregate
kennung.fs     10000     220     2%    34% = 4217460/12331384 (LFS)
```

Diese Zeilen besagen, daß für das *Fileset* `kennung.fs` eine *Quota* von 10000 KB gilt, daß davon 220 KB, also etwa 2 % der *Quota*, genutzt sind, daß das *Fileset* sich in einem als *Local File Store (LFS)* organisierten *Aggregate* der Größe 12331384 KB (etwa 12 GB) befindet, von welchem 4217460 KB, also etwa 34 %, belegt sind.

Sollten Sie mit Ihrer *Quota* nicht auskommen (Fehlermeldung *Quota exceeded*) oder sollte gar – was selbst bei nicht ausgenutzter *Quota* geschehen kann – das *Aggregate* voll sein (Fehlermeldung *disk full*), dann wenden Sie sich bitte an die Unix-Systemgruppe (✆ `urz@uni-muenster.de`), die Ihre *Quota* anpassen oder Ihr *Fileset* in ein anderes *Aggregate* verschieben kann.

In anderen Punkten verhalten sich *Filesets* wie herkömmliche Dateisysteme, insbesondere sind *Hardlinks* nur innerhalb eines *Filesets*, nicht aber zwischen Dateien verschiedener *Filesets* möglich.

Sicherheitstechnisch gelten in DFS-Filesets die Schutzmechanismen (*Access Control Lists*) des DCE, nicht die herkömmlichen Unix-Dateischutzmechanismen. Dies hat zur Folge, daß der Befehl `umask` und in der Regel auch die `setuid`- und `setgid`-Bits wirkungslos sind und daß die Befehle `chmod`, `ls -l`, `find`

usw. insbesondere in Bezug auf die *Group-Permission*-Bits geringfügig anders funktionieren.

Die neuen Schutzmechanismen erfordern bei der Verwendung des Druckbefehls `enq` die Angabe der Option `-c` sowie bei den Befehlen `lpr`, `p3800` oder `lprint` den Verzicht auf die Option `-s`, da sonst der Druckprozeß nicht mehr auf die zu druckende Datei zugreifen kann.

Neuer E-Mail-Server

R. Perske

Rasant wachsende Nutzungszahlen machten einen weiteren Ausbau der E-Mail-Dienste erforderlich.

Unsere zentralen E-Mail-Server arbeiten im wesentlichen mit drei verschiedenen Internet-Protokollen:

- **SMTP** (*Simple Mail Transport Protocol*) dient zum Versenden, Transportieren und Zustellen von E-Mail.
- **POP3** (*Post Office Protocol Version 3*) dient zum Abholen zugestellter E-Mail.
- **IMAP** (*Internet Message Access Protocol*) dient zum Abholen und Verwalten zugestellter E-Mail.

Nachdem die explosionsartig steigende Zahl der POP3- und IMAP-Anforderungen an den zentralen E-Mail-Server die Leistungsgrenze der erst kürzlich installierten Maschine schon wieder überschritten und damit auch E-Mail-Transport und -Zustellung behindert hatten, konnte die Last Ende Juni auf zwei Rechner verteilt werden.

Die bisherige Maschine `mail` dient weiterhin als SMTP-Server und besorgt Annahme, Weiterleitung und Zustellung der E-Mail.

Die neu beschaffte Maschine `pop1` vom Typ RS/6000 Model 43P-240 ist mit ihren zwei mit 233 MHz getakteten PowerPC-604-Prozessoren der schnellste Rechner des Universitätsrechenzentrums und dient jetzt als POP3- und IMAP-Server zum Abholen eingegangener E-Mail.

Durch die Trennung der Serverfunktionen haben hohe Nachfragezahlen nach eingegangener E-Mail keinen negativen Einfluß mehr auf E-Mail-Annahme, -Transport und -Zustellung.

Die explodierenden Nutzungszahlen lassen erwarten, daß selbst der neue POP3- und IMAP-Server in absehbarer Zeit an seiner Leistungsgrenze ankommen wird. Dann kann jedoch ohne technische Probleme die Last auf mehrere POP3- und IMAP-Server verteilt werden.

Wegen dieser Aufteilung müssen POP3- und IMAP-Nutzer, die bislang noch `mail.uni-muenster.de` als Server eingetragen hatten, spätestens jetzt ihre E-Mail-Konfiguration in Ordnung bringen:

SMTP-Server	`mail.uni-muenster.de`
POP3-Server	`pop.uni-muenster.de`
IMAP-Server	`imap.uni-muenster.de`

Tragen Sie bitte keinesfalls andere Namen ein, auch wenn diese derzeit noch funktionieren mögen.

Bei der Umstellung trat ein Problem mit der neu eingesetzten POP3-Software auf, das zu sporadischen Rechnerabstürzen beim Abholen übergroßer E-Mails führte. Durch Zurückschalten auf die bisherige POP3-Software konnte das Problem umgangen werden.

Die neue POP3- und IMAP-Software hat den Nebeneffekt, daß viele Nutzer eine E-Mail wie die folgende zu sehen bekommen:

```
From: Mail System Internal Data <MAILER-DAEMON@pop1.uni-muenster.de>
Subject: DON'T DELETE THIS MESSAGE -- FOLDER INTERNAL DATA

This message contains status data for IMAP and POP servers.
```

Diese Pseudomail wird von der neuen Software angelegt, um Statusinformationen aufzubewahren. Man sieht diese Mail dann, wenn man, nachdem man die neue Software genutzt hat, wieder entweder die alte Software nutzt oder direkt auf die Mailboxdatei im Unix-Verzeichnis `/var/spool/mail` zugreift.

Ein Löschen dieser Mail ist ungefährlich, es gehen nur die vom IMAP-Server verwalteten Informationen verloren, welche Mails bzw. Mailteile bereits gelesen wurden.

Für Nutzer des E-Mail-Programms `pine` unter Unix wird es in diesen Tagen eine Änderung geben: Die Konfiguration wird so geändert, daß nicht mehr direkt auf die Mailboxdatei, sondern über IMAP auf eingegangene E-Mails zugegriffen wird. Wundern Sie sich also bitte nicht, wenn Sie beim Lesen von E-Mail plötzlich nach Ihrem Paßwort gefragt werden!

Zur Situation der Einwählzugänge

G. Richter

Beim Testen neuer Einwählzugänge vom häuslichen Arbeitsplatz ins Universitätsrechenzentrum bitten wir unsere Nutzer um Mithilfe.

Aufgrund der erheblichen technischen Schwierigkeiten der Einwählzugänge unter der Rufnummer 981521, aufgrund des weitaus höheren Bedarf als derzeit durch die vorhandenen 60 Modem-Kanäle abgedeckt und aufgrund des zusätzlichen Bedarfs an ISDN-Einwählzugängen arbeitet die Gruppe Kommunikationssysteme im Universitätsrechenzentrum mit hoher Priorität an einer grundsätzlichen Umstrukturierung der Netz- und Systemzugänge über Einwählleitungen. Insbesondere soll der bisherige Zugang über Unix-Systeme (comix) abgelöst werden durch dedizierte Spezialgeräte, die z. B. auch durch ISPs (*Internet Service Provider*) verwendet werden.

Folgende Zugänge sind deshalb zur Zeit im Evaluations-/Testbetrieb bzw. sind als Vorablösung installiert.

I. **Analog-Zugang** Rufnummer (0251) 981561
(USR Total Control):

Bereits seit einigen Wochen befindet sich ein System der Fa. US Robotics (USR Total Control) mit weitgehend großem Erfolg im Testbetrieb. Aus diesem Grunde wurden bereits 30 Kanäle freigeschaltet; die Zahl der Zugänge unter 981521 wurde entsprechend auf 30 verringert.

Folgende Zugangsverfahren sind im Rahmen des Testbetriebs mit dem Total-Control-System möglich:

1. PPP-Sitzung über Terminal-Anmeldung:

   Das System sendet eine `login`-Zeichenkette, nach Authentifizierung in einem Terminalfenster erfolgt sofort die PPP-Negotiation. Ein Starten eines `pppd`-Programmes auf dem Einwählsystem wie bisher ist nicht mehr erforderlich; auf dem einwählenden System ist der *Packet Mode*, d. h. PPP, ggf. zu starten – in der Regel erfolgt dies jedoch automatisch.

2. PPP-Sitzung über PAP:

   PPP-Anmeldung ohne Terminalfenster, PPP-Negotiation und Authentifizierung über PAP-Methode innerhalb des Wählprogramms des einwählenden Rechners. Diese Methode wird beispielsweise von Windows 95 und Windows NT unterstützt. Dies ist die empfohlene Methode; ein Login-Script ist hierbei nicht notwendig.

3. Terminalsitzung ohne PPP:

   Login erfolgt wie unter 1., jedoch ist die Nutzerkennung mit angehängtem „+“ (z. B. `richter+`) einzugeben, und es ist die Angabe des Zielrechners für eine Terminalsitzung notwendig.

   Dieses Verfahren ist nur noch für Nutzer sinnvoll, die keine TCP/IP- bzw. PPP-Software verwenden können (z. B. bei MSDOS-Altsystemen)

.

Anleitungen für diverse DFÜ-Software sind in Arbeit. Die Authentifizierung erfolgt mit den Nutzerkennungen des Universitätsrechenzentrums im Rahmen der Authentifizierungssysteme der AIX-Unix-Rechner (DCE).

Das System unterstützt z. Z. maximal 33,6 kBaud. Der Einsatz von schnelleren Verfahren (z. B. X2) ist noch nicht möglich; ggf. kann dies zu einem späteren Zeitpunkt erfolgen.

Eine zeitliche Beschränkung dieses Testbetriebs ist bisher nicht vorgesehen, jedoch behalten wir uns für den Notfall vor, den Testbetrieb nach Vorankündigung zu beenden und den Betrieb ohne Vorankündigung kurzzeitig zu unterbrechen. Im Grundsatz besteht die Absicht, dieses System baldmöglichst in den Regelbetrieb zu überführen und weiter auszubauen.

II. ISDN-Zugang Rufnummer (0251) 981561
(USR Total Control):

Das unter I. genannte USR-Total-Control-Zugangssystem ist nach Angaben des Herstellers auch für den ISDN-Zugang geeignet. Erfahrungen liegen bisher nicht vor. Ab ca. Ende Juli 1997 soll ein erster ISDN-Testbetrieb beginnen, der jederzeit ohne Vorankündigung wieder beendet werden kann. Weitere Informationen erfolgen baldmöglichst.

III. ISDN-Zugang Rufnummern (0251) 9814-23, -24, -33
(Terminaladapter an `comix`):

Als Vorablösung für einen ISDN-Zugang sind seit längerem 3 Terminaladapter (TA), d. h. also 6 B-Kanäle, unter obengenannten Rufnummern installiert.

Die TAs sind an die `comix`-Systeme wie die bisherigen analogen Modems mit 57600 Bit/s angeschlossen. Es gelten also die gleichen Verhältnisse wie bei den Modems. Diese „ISDN-Modems“ unterstützen das Protokoll X.75/transparent für den ISDN-B-Kanal.

Manche Hersteller von ISDN-Karten bieten neben der CAPI-Software noch einen sog. COM-Emulator (z. B. Teles, S0-Karte, SW unter Windows). Damit lassen sich auch PPP-Verbindungen wie bei den bisherigen analogen Modemzugängen (`comix`) herstellen.

Diese Terminaladapter werden wegfallen, sobald ein Regelbetrieb mit ISDN bereitgestellt werden kann.

IV. ISDN-Zugang Rufnummern (0251) 800-22, -20
sowie universitätsintern (0251) 83-315-54, -56, -57, -58
(3Com Accessbuilder 4000):

Als Vorablösung für einen ISDN-Zugang ist seit einiger Zeit ein dediziertes System der Fa. 3Com (Accessbuilder 4000) mit insgesamt 12 ISDN-B-Kanälen im beschränkten Testeinsatz.

Der Zugang erfolgt über synchrones PPP über den ISDN-B-Kanal (HDLC transparent).

Zur Benutzung dieses Testzugangs ist es im Moment erforderlich, daß Sie in

der Windows-NT-Domäne WWU des Universitätsrechenzentrums eine Kennung besitzen. Wenn Sie den Testzugang benutzen wollen, melden Sie sich bitte bei der PC-Systemgruppe:

Herr M. Kämmerer (✆ 31657, @ kammere@uni-muenster.de),
Herr M. Kamp (✆ 31658, @ kampm@uni-muenster.de),
Herr Dr. W. Lange (✆ 31655, @ lange@uni-muenster.de).

Eine Integration in die allgemeine Nutzer-Authentifizierung ist z. Z. noch nicht möglich. Die Überführung in die DCE-Authentifizierung der URZ-Unix-Systeme soll mit dem nächsten Software-Release erfolgen.

Der Testbetrieb kann nach Vorankündigung eingestellt werden, voraussichtlich jedoch erst dann, wenn der ISDN-Regelbetrieb aufgenommen worden ist.

V. ISDN-Zugang Rufnummer (0251) 981591
(3Com Accessbuilder 5000)

Im Rahmen der Evaluation von Einwählsystemen wird das URZ ca. ab Ende Juli 1997 ein Einwählsystem der Fa. 3Com (Accessbuilder 5000) mit 30 ISDN-B-Kanälen testen. Die Eigenschaften sollen denen des Accessbuilder 4000 (s. IV.) weitgehend gleichen, jedoch wird für die Authentifizierung keine besondere Kennung in der NT-Domäne notwendig sein und alle 30 Kanäle werden über eine Rufnummer angewählt werden können. Der Testbetrieb ist zunächst auf ca. 6 Wochen beschränkt.

Testbetriebsunterbrechungen werden auch ohne Vorankündigung im Notfall durchgeführt werden müssen. Weitere Informationen erfolgen baldmöglichst in den aktuellen Nachrichten des URZ (NetNews-Forum wwu.dv.kommunikation.ppp bzw. WWW-Seiten des URZ).

Alle genannten Testzugänge dienen dem Auswahlverfahren für Einwählsysteme. Eine Gewährleistung für eine längere Weiterführung oder die Stabilität des Testbetriebes kann deshalb nicht gegeben werden; man muß jederzeit mit unangekündigten Störungen rechnen. Bitte beteiligen Sie sich nach Möglichkeit trotzdem an den Tests, denn für eine qualifizierte Auswahl ist es notwendig regelbetriebsähnliche Verhältnisse (Lastaufkommen, große Nutzerzahlen) zu erhalten.

Die Zuordnung der Rufnummern für die genannten Zugänge ist noch vorläufig; schließen Sie bitte also keine Rabattierungsverträge für diese von Ihnen möglicherweise häufig genutzten Zugänge ab.

Ihre Erfahrungsberichte sind willkommen (Erfolgsmeldungen oder Problemberichte). Insbesondere der Testbetrieb entsprechend I., II. und V. erscheint für die Zukunft von erheblicher Bedeutung; die Zugangsvarianten III. und IV. dienen eher denjenigen, die heute bereits auf ISDN-Zugänge angewiesen sind.

Möglichst detaillierte, auswertbare Erfahrungsberichte werden erbeten an unser *Network Operating Center* (noc@uni-muenster.de).

Je mehr und je schneller Erfahrungen zusammengetragen werden können, um so eher wird es uns möglich sein, den Testbetrieb in einen Regelbetrieb zu überführen. Für Ihre Kooperation danken wir im voraus.

Netzprobleme bei mangelnder Qualität von Anschlußkabeln

G. Richter

Beim Anschluß von Rechnern an das lokale Rechnernetz der Universität sollten keine beliebigen Kabel verwendet werden.

Bereits mehrfach haben Nutzer des lokalen Rechnernetzes (LAN) durch eigene Erfahrungen lernen müssen, daß nicht jedes beliebige Kabel, auch wenn es steckerkompatibel aussieht, für die Verbindung eines Rechners mit einer LAN-Anschlußdose geeignet ist. Der lokale Handel bietet solche „steckerkompatiblen" Kabel an. Die Erfahrung ist dann häufig, daß der Rechner gar nicht oder nur mit geringem Durchsatz im Netz betrieben werden kann. Dabei entgeht dem Nutzer teilweise noch, daß andere Netzbenutzer – durch ebenfalls verminderten Durchsatz an deren Rechnern – massiv beeinträchtigt werden. Die Lokalisierung solcher Fehlerquellen hat die Nutzer und das Universitätsrechenzentrum bereits erheblichen zeitlichen Aufwand gekostet, da solche Fehlerquellen zunächst gar nicht bedacht werden, zumal das Universitätsrechenzentrum geeignete Kabel in großem Umfang vorhält und zu günstigen Preisen an die Nutzer ausgibt.

Darüber hinaus muß damit gerechnet werden, daß der Betrieb eines ungeeigneten Kabels zu unzulässigen elektromagnetischen Emissionen führt, die die gesetzlich erlaubten Grenzwerte weit überschreiten und beispielsweise den Funkverkehr stören. Dies gilt sowohl für Anschlüsse mit 100 MBit/s (Fast Ethernet und „Kupfer-FDDI") als auch für die zunächst weniger kritisch erscheinenden Anschlüsse mit „nur" 10 MBit/s (Ethernet auf Twisted-Pair-Kabeln, 10BaseT).

Der Betreiber eines Rechnernetzes ist rechtlich für die Einhaltung der einschlägigen EMV-Gesetze (EMV = elektromagnetische Verträglichkeit) verantwortlich. Hier kann nicht erörtert werden, wer im Falle eines Falles die Konsequenzen letztendlich zu tragen hätte; das Universitätsrechenzentrum ist nach der geltenden Betriebsregelung für das Rechnernetz allerdings verantwortlich für die Signaltechnik und dazu gehört zweifelsfrei das Übertragungskabel im allgemeinen und das Anschlußkabel im besonderen.

Das Universitätsrechenzentrum bittet deshalb alle Betreiber von Rechnern im LAN, ihre Anschlußkabel ausschließlich über das Universitätsrechenzentrum zu beziehen. Der Nutzer kann dann weitgehend davon ausgehen, daß das Kabel einwandfrei funktioniert und niemand anders (im LAN oder durch elektromagnetische Emissionen) beeinträchtigt wird. Das Universitätsrechenzentrum sorgt dafür, daß einwandfrei spezifizierte Kabel bestellt werden; durch Großeinkauf unter Wettbewerbsbedingungen kann der Preis sehr günstig gehalten werden. Kabel können bei Herrn Mohr oder Herrn Focke (✆ 31650 bzw. ✆ 31667), Gebäude Röntgenstr. 13, möglichst nach vorheriger Anmeldung und unter Vorlage eines Bestellscheines, abgeholt werden.

RUM-Tutorial

Das Urheberrecht an Computersoftware – Hinweise für Anwender

Dr. St. Ernst

Aus dem hier abgedruckten Artikel kann gegenüber der infoRUM-Redaktion kein Rechtsanspruch abgeleitet werden. Allein der Autor steht für die hier gemachten Aussagen gerade.

Warum Urheberrecht und wer besitzt es

Dieser Text will dem juristischen Laien einen kurzen und schnellen Überblick über das Computerurheberrecht geben, das im wesentlichen im Urheberrechtsgesetz (UrhG) geregelt ist. Daß hierbei nicht alle Einzelfragen behandelt werden können, ist offenbar. In Zweifelsfällen, insbesondere bei Vorhandensein gegenläufiger Vertragsklauseln, sei dem Anwender daher empfohlen, anwaltlichen Rechtsrat einzuholen.

Die Existenz des Urheberrechts an Software ist schnell und einleuchtend begründet. Wer ein Computerprogramm schreibt bzw. schreiben läßt, muß – je nach Programm – sehr viel Aufwand betreiben. In umfangreichen Softwaresystemen steckt viel Geld, so daß es nur verständlich erscheint, wenn der Unternehmer, der dieses Geld investiert hat, das Programm lieber verkauft als verschenkt. Da das Kopieren von Software einfach ist, erscheint die Rentabilität von aufwendigen Softwareprodukten gefährdet. Deshalb sind Computerprogramme als geistiges Eigentum durch das Urheberrecht geschützt. Es besteht unter Fachjuristen zwar Uneinigkeit, ob ein gewerbliches Schutzrecht (z. B. ein Patent) nicht sachgerechter gewesen wäre, weil das Urheberrecht von seiner Natur her nur kulturelle Arbeiten betrifft, doch hat der Gesetzgeber nun einmal diesen Weg gewählt. Bedeutung hat dies für den Schutz insofern, als das Urheberrecht auch ohne eine besondere Anmeldung beim Patentamt und ohne eine Kennzeichnung durch Zeichen wie © besteht. Copyright-Hinweise auf CD oder Verpackung sind insofern also rein deklaratorisch.

Urheber ist grundsätzlich der Schöpfer des Werkes. Dies ist bei Software der Programmierer. Da aber die meisten Programme von angestellten Arbeitnehmern im Rahmen ihrer Arbeit geschaffen werden, wird im Regelfall der Arbeitgeber zur Ausübung der Rechte befugt sein. Das Gesetz hat diesen Fall besonders geregelt. § 69b UrhG weist dem Arbeitgeber die Ausübung aller vermögensrechtlichen Befugnisse aus dem Softwareurheberrecht zu. Auch wenn die Programmierer (es werden wohl meist mehrere sein) formal Urheber bleiben, so ergibt sich für sie aus dieser Stellung kein nennenswerter Vorteil.

Der Schutz von Programmen ist im übrigen unabhängig von ihrem qualitativen oder auch ästhetischen Gehalt. Das Urheberrecht schützt auch die sog. „kleine Münze“, d. h. Programme von geringer schöpferischer Leistung (§ 69a Abs. 3 UrhG). Ideen und Grundsätze, die einem Element des Programms zugrunde liegen, sind hingegen frei (§ 69a Abs. 2 UrhG).

Wo beginnt die Raubkopie

Für den Anwender von Computersoftware bedeutet dies, daß die Verwendung von Software grundsätzlich den Erwerb eines Nutzungsrechts voraussetzt. Der Urheber hat gem. § 69c UrhG das ausschließliche Recht zur Vervielfältigung, Ver-

breitung und Bearbeitung. Das bedeutet: Benutzen, Kopieren, Verkaufen, Verschenken, Vermieten oder Verändern des Programmes muß erst erlaubt werden. Dies wird im Normalfall natürlich nicht über ein persönliches Gespräch zwischen User und Urheber, sondern über den Kauf von Software beim vom Urheber beauftragten Softwarehändler geschehen. Urheberrechtlich erwirbt der Anwender hierdurch eine Nutzungslizenz. Eine solche Nutzungslizenz kann beschränkt sein. Sie berechtigt, wenn nicht ausdrücklich eine Mehrplatzlizenz vergeben wird, nur zur Benutzung des Programms auf einem Einplatzrechner. Jede Kopie, die über die vereinbarte Benutzung hinaus angefertigt wird, ist eine unzulässige Kopie, die das Urheberrecht verletzt.

Eigenmächtige Änderungen an Software

Änderungen am Programm sind ohne Erlaubnis nur zur Fehlerberichtigung zulässig (§ 69d Abs. 1 UrhG). Damit unterscheiden sich Computerprogramme von anderen urheberrechtlich geschützten Werken. Als Eigentümer eines Gemäldes darf ich dieses verändern, solange ich diese Veränderung nicht veröffentliche oder gar verkaufe. Dies gilt nicht für Software. Hier ist schon das Herstellen einer Umarbeitung von der vorherigen Zustimmung des Urheberrechtsberechtigten abhängig.

Ausprobieren von Software

Rechtlich relevant ist bereits das bloße Aufrufen eines Programms. Auch dies ist vom Urheberrecht umfaßt, denn eine Vervielfältigung im Sinne des § 69c UrhG muß nicht dauerhaft sein. Eine urheberrechtlich relevante Handlung liegt schon dann vor, wenn das Programm zur Nutzung in den Arbeitsspeicher kopiert wird. Das Sharewarekonzept entstand gerade aus dieser Problematik heraus, daß der Nutzer im Prinzip gezwungen war, die Katze im Sack zu kaufen, ohne zu wissen, ob die Software die gewünschten Leistungen erbringt.

Einsatz auf mehreren Rechnern

Wer ein Programm kauft, erwirbt, wenn nicht ausdrücklich eine Mehrplatzlizenz vergeben wird, das Recht zur Nutzung auf einem einzelnen Computer. Er darf die Software also ohne besondere Gestattung (und Bezahlung) nicht in einem Mehrplatzsystem einsetzen. Auch ist er nicht berechtigt, das Programm auf alle Rechner des Hauses zu kopieren, obwohl sich dies in einigen Wohngemeinschaften und sogar in kleineren Unternehmen eingebürgert hat. Wird in einer Lizenz eine Zahl von zulässigen Arbeitsplätzen vereinbart, ist diese bindend. Jede Kopie, die über die vereinbarte Zahl hinausgeht, verletzt das Urheberrecht. Dies gilt auch, wenn wegen Überlastung durch einen Kurs kurzzeitig der Wunsch nach weitere Kopien besteht.

Dies gilt grundsätzlich auch für Personen, die einerseits zu Hause oder im Büro einen Desktop nutzen und andererseits einen Laptop zur gelegentlichen Outdoor-Nutzung bereithalten. Soll dasselbe Programm auf beiden Rechnern benutzt werden, sind zwei Lizenzen zu erwerben. Alternative wäre das Löschen des Programms auf dem einen Rechner, bevor es auf dem anderen (wieder) installiert wird. Dies mag lächerlich erscheinen, ist aber urheberrechtlich geboten.

Wer ein rechtmäßig erworbenes Softwareprodukt weiterverkauft oder verschenkt, muß alle bei ihm vorhandenen Kopien löschen.

Sicherungskopien

Die Erstellung einer Sicherungskopie ist hingegen erlaubt und kann auch nicht vertraglich untersagt werden, sofern diese für die Sicherung künftiger Benutzung erforderlich ist (§ 69d Abs. 2 UrhG). Kauft also z. B. der Benutzer einen Rechner mit vorinstallierter Software, so darf er sich zur Sicherung dieser Programme (und nur dafür!) eine Kopie auf Diskette ziehen.

Keine „privaten“ Kopien

Wem das Recht zur privaten Kopie etwa von Musikaufnahmen oder einzelner Zeitschriftenaufsätze aus § 53 UrhG bekannt ist, muß wissen, daß dieses Recht sich nicht auf Computerprogramme erstreckt. Den Urheberinteressen wird in den beiden genannten Beispielen dadurch Rechnung getragen, daß jeder Verkauf einer leeren MC (DM 0,12/h) oder einer Videokassette (DM 0,17/h), eines Kassetten- (DM 2,50) oder Videorecorders (DM 18.-) den entsprechenden Urhebern über Verwertungsgesellschaften wie der GEMA ebenso bares Geld bringt wie jede Fotokopie in einem Copyshop (DM 0,02). Daß dies bei Software nicht möglich ist, erscheint offenbar. Das auf eine Musikkassette kopierte Original, in einer Leerkassette vergütet mit DM 0,12, kostet im Handel maximal DM 40,–. Eine kopierte Diskette oder CD hingegen kann theoretisch Software für DM 4000,– aufnehmen, so daß vernünftige Vergütungssätze nicht möglich sind.

Freeware, Public-Domain, Shareware

Die Nutzung von Freeware oder Public-Domain-Produkten ist urheberrechtlich unbedenklich. Bei Shareware-Produkten hingegen ist die Nutzung durch die sharewarespezifische Nutzungslizenz begrenzt. Der Nutzer besitzt eine zeitlich begrenzte Gestattung und muß das Programm nach Ablauf der Frist von seinem Rechner entfernen. Tut er dies nicht, verstößt auch er gegen das Urheberrecht. Was passiert bei Gesetzesverstößen? Das Erstellen, Vertreiben und Benutzen von Raubkopien kann strafrechtliche Konsequenzen nach sich ziehen (§§ 106 ff. UrhG). Das UrhG bedroht sogar den Versuch mit einer Strafe, die bei gewerbsmäßigem Handeln noch empfindlich erhöht werden kann. Gewerbsmäßig bedeutet ein wiederholtes Handeln, das zu einer (Neben-)Einnahmequelle von einiger Dauer und einigem Umfang führt. Die zivilrechtlichen Folgen (§ 97 UrhG) können, da finanziell oft erheblich bedeutender, für den Täter noch weitaus unangenehmer werden. Die Schadensersatzzahlungen einschließlich der Anwaltsgebühren der Softwarefirma, die mitzutragen sind, können sich je nach Umfang der Tat im vier- bis fünfstelligen Bereich bewegen. Alle Raubkopien können vernichtet werden (§ 69f UrhG).

Raubkopien im Internet

Im Urheberrecht gilt das Territorialprinzip. Das bedeutet, daß bei Urheberrechtsverletzungen das Recht des Landes angewandt wird, in dem das Urheberrecht verletzt wurde. Dort kann auch geklagt werden. Bedeutung hat dies in ganz besonderer Weise für die Verbreitung von Raubkopien über das Internet. Ort der Urheberrechtsverletzung ist nicht nur der Ort, wo die Raubkopie eingespeist wurde, sondern jeder Ort, wo sie bestimmungsgemäß abrufbar ist. Da das Internet ubiquitär ist, findet die Verletzungshandlung also praktisch überall statt, was (neben den deutschen) auch die Zuständigkeit etwa US-amerikanischer Gerichte begründen würde. Ausländische Urteile sind dabei grundsätzlich auch in Deutschland vollstreckbar. Wer sich umgekehrt eine Raubkopie aus dem Netz holt, dürfte hingegen wohl nur in Deutschland verurteilt werden können, da der Handlungs- und Erfolgsort hier liegt.

Kryptografische Fingerabdrücke

R. Perske

Sichere Datenübertragung im Internet erfordert den Einsatz kryptografischer Methoden. Mit Hilfe relativ kurzer Ziffernfolgen kann man kontrollieren, ob ein verwendeter Schlüssel tatsächlich zum angegebenen Besitzer gehört.

Die durch das Internet laufenden Daten sind besonderen Gefahren ausgesetzt: Ohne große Probleme können die Datenströme abgehört, umgeleitet, unterbrochen, verfälscht oder sonstwie gestört werden. Durch Anwendung kryptografischer Methoden kann jedoch ein gewisses Maß an Sicherheit erreicht werden.

Public Keys – Wie funktioniert das?

Bereits im Artikel „Sicheres World Wide Web“ im infoRUM Nr. 3/1996 wurden die Kernfragen angesprochen. Angenommen, Hans sendet Otto eine Nachricht:

- Woher weiß Otto, daß die Nachricht wirklich von Hans stammt und unterwegs nicht verfälscht wurde? (Stichwort Digitale Unterschrift)
- Wie stellt Hans sicher, daß die Nachricht nur von Otto gelesen werden kann? (Stichwort Verschlüsselung)
- Wie stellt Hans sicher, daß seine Nachricht auch bei Otto ankommt?

Während Hans und Otto als normale Internet-Nutzer meist keinen Einfluß auf die Stabilität einer Verbindung haben und somit nie sicher sein können, daß die Nachricht auch ankommt, können sie die ersten beiden Probleme mit sogenannten *Public-Key*-Verfahren lösen.

Bei diesen hier vereinfacht dargestellten Verfahren erzeugt sich jeder der beliebig vielen Teilnehmer zwei zueinander passende Schlüssel. Daten, die mit einem der beiden Schlüssel verschlüsselt wurden, können nur mit dem jeweils anderen Schlüssel wieder entschlüsselt werden.

Während jeder Teilnehmer einen der beiden Schlüssel sorgfältig geheim halten muß, kann und sollte er – was bei herkömmlichen Verfahren völlig undenkbar wäre – den anderen Schlüssel veröffentlichen, so daß jeder Interessierte darauf

zugreifen kann. Daher kommt der Name *Public Key*. Zu jedem Teilnehmer gehören also ein geheimer und ein öffentlicher Schlüssel.

Wenn Hans jetzt Otto eine vertrauliche Nachricht senden möchte, verschlüsselt er die Nachricht mit dem öffentlichen Schlüssel von Otto. Dann kann nur Otto, der als einziger seinen geheimen Schlüssel kennt, die Nachricht wieder entschlüsseln. Nicht einmal Hans selbst ist dazu noch in der Lage.

Wenn Hans jetzt Otto eine Nachricht so senden möchte, daß Otto Herkunft und Richtigkeit der Nachricht kontrollieren kann, dann verschlüsselt er eine aus der Nachricht gebildete Prüfsumme mit seinem eigenen geheimen Schlüssel, d. h. er unterschreibt sie. Er sendet dann sowohl die Nachricht als auch die verschlüsselte Prüfsumme an Otto. Dann kann Otto die Prüfsumme mit Hans' öffentlichem Schlüssel entschlüsseln und mit der Nachricht vergleichen und sieht so, ob die Nachricht von Hans stammt und nicht verändert wurde.

(Dazu muß man natürlich ein kryptografisch sicheres Prüfsummenverfahren verwenden, also ein Verfahren, bei dem es praktisch unmöglich ist, eine zweite Nachricht mit der gleichen Prüfsumme zu finden.)

Beide Verfahren lassen sich selbstverständlich kombinieren.

Dabei stellt sich dann allerdings ein Folgeproblem:

- Woher weiß Hans, daß Ottos öffentlicher Schlüssel wirklich von Otto stammt, und umgekehrt? (Stichwort Zertifizierung)

Die simple Lösung, sich den Schlüssel von Otto persönlich geben zu lassen und dabei seinen Ausweis einzusehen, ist nicht immer durchführbar. Falls Hans aber Otto an der Stimme erkennt, kann er sich Ottos öffentlichen Schlüssel von Otto vorlesen lassen.

Das ist bei den langen Ziffernkolonnen, aus denen die Schlüssel der Public-Key-Verfahren bestehen, natürlich sehr umständlich. Es reicht aber, wenn Hans sich den Schlüssel anderweitig besorgt und eine Prüfsumme daraus bildet. Otto braucht von seinem Schlüssel nur ebenfalls die Prüfsumme zu bilden und diese telefonisch an Hans durchgeben. Wenn die Prüfsummen übereinstimmen, kann Hans schon sicher sein.

(Auch hierzu muß man wiederum ein kryptografisch sicheres Prüfsummenverfahren verwenden.)

Diese praktisch nicht nachahmbare Prüfsumme eines Schlüssels nennt man auch seinen Fingerabdruck oder auf englisch *finger print*.

Zertifikate – Wie funktioniert das?

Wenn Hans und Otto sich aber gegenseitig nicht kennen und auch nicht treffen können, benötigen sie eine oder mehrere Stellen, die ihnen die öffentlichen Schlüssel beglaubigen.

Angenommen, Hugo besitzt das nötige Vertrauen von Hans, Otto und vielen anderen. Dann könnte Otto (wie jeder andere auch) sich irgendwann mit Hugo treffen, sich ausweisen und seinen öffentlichen Schlüssel vorlegen. Hugo würde dann seinen eigenen geheimen Schlüssel verwenden, um ein *Zertifikat* für Ottos öffentlichen Schlüssel auszustellen. So ein Zertifikat ist im Prinzip ein unter-

schriebenes Dokument, in dem bestätigt wird, daß der öffentliche Schlüssel zu einer bestimmten Person gehört. Otto und die anderen würden dann nicht nur die öffentlichen Schlüssel, sondern auch die zugehörigen Zertifikate veröffentlichen.

Hans kann jetzt kontrollieren, ob ein fragwürdiger öffentlicher Schlüssel zu Otto gehört, indem er einerseits obiges Zertifikat mit Hugos öffentlichem Schlüssel überprüft und andererseits den fragwürdigen Schlüssel mit diesem Zertifikat vergleicht. Solange Hugo keine falschen Zertifikate ausstellt, kann Hans sicher sein, daß der fragwürdige Schlüssel zu Otto gehört.

Auch von so einem Zertifikat kann man einen Fingerabdruck bilden. Falls Hans den öffentlichen Schlüssel von Hugo noch nicht überprüft oder erst gar nicht zur Hand hat, kann er Hugo anrufen, sich den Fingerabdruck des Zertifikats vorlesen lassen und so überprüfen, ob das Zertifikat gültig ist.

Public Keys im Universitätsrechenzentrum

Das Universitätsrechenzentrum setzt Public-Key-Verfahren derzeit einerseits bei den abhörsicheren WWW-Servern ein, die beispielsweise zur Paßwortänderung verwendet werden, und andererseits zunehmend auch im Bereich der elektronischen Post und der elektronischen Konferenzen.

Public Keys im World Wide Web

Die für den Anwender ziemlich verborgene Anwendung der Public Keys bei unseren abhörsicheren WWW-Servern wurde schon im Artikel „Sicheres World Wide Web“ im infoRUM Nr. 3/1996 beschrieben. Wie dort schon vorhergesagt, haben wir jetzt die Schlüssel und die Zertifikate unserer WWW-Server geändert. Mit Hilfe des jeweiligen Fingerabdrucks können Sie überprüfen, ob das Zertifikat für die Identität eines jeweiligen WWW-Servers tatsächlich von mir ausgestellt wurde.

Solange Sie das nicht getan haben, wird Ihr Browser Ihnen beim Zugriff auf unsere abhörsicheren WWW-Seiten mitteilen, daß er die *authority*, die das Zertifikat ausgestellt habe, nicht kenne. Beim Netscape Navigator ab Version 2 können Sie dann selbst anhand des Fingerabdrucks entscheiden, ob Sie das Zertifikat akzeptieren möchten, manch anderer verbreiteter Browser bietet Ihnen diese Chance leider nicht.

(Die Abhörsicherheit wird bei den WWW-Browsern allerdings nicht durch ein Public-Key-Verfahren, sondern durch ein herkömmliches Verschlüsselungsverfahren erreicht. Das Public-Key-Verfahren dient nur zum Identitätsnachweis und zur sicheren Übertragung des vom Client erzeugten Schlüssels zum Server. Daher braucht auch nur der Server einen geheimen Schlüssel.)

Die Fingerabdrücke der aktuell gültigen Zertifikate lauten:

```
mail.uni-muenster.de: 91 73 A4 91 77 A0 CD 5A BF 22 AD C0 FE 5A 3D 67
www.uni-muenster.de:  D0 B9 D4 0A 47 C3 BE 7D A9 2E DA BB BB 56 1A CB
```

Diese Zertifikate haben folgende Daten als Herausgeber eingetragen:

```
Rainer Perske; perske@uni-muenster.de; Universitätsrechenzentrum;
Westfälische Wilhelms-Universität Münster; Münster; Germany; DE.
```

Public Keys bei E-Mail und NetNews

Wie schon viele unserer Nutzer haben auch einige Mitarbeiter des Universitätsrechenzentrums begonnen, ihre per E-Mail verschickten oder in den NetNews veröffentlichten Mitteilungen elektronisch zu unterschreiben und in manchen Fällen auch zu verschlüsseln. Sie benutzen dazu das ebenfalls im genannten Artikel erwähnte Programmpaket PGP (*Pretty Good Privacy*), welches unter anderem auf den vom Universitätsrechenzentrum betreuten Unix-Systemen installiert ist.

Nutzer des auf den gleichen Systemen installierten E-Mail- und Net-News-Programms `pine` können durch eine relativ einfache Konfigurationsänderung ebenfalls mit der Nutzung von PGP beginnen. Diese Änderungen sind im World Wide Web auf der Seite `http://www.uni-muenster.de/URZ/Hinweise/PGPmitPine.html` veröffentlicht.

Sie sollten aber erst mit der Nutzung von PGP beginnen, wenn Sie die von dieser Seite aus erreichbare Dokumentation gelesen *und verstanden* haben, ansonsten könnten Sie sich durch leichtfertigen Umgang in falscher Sicherheit wiegen. Weitere Informationen zu PGP finden Sie auf der internationalen PGP-Home-Page `http://www.ifi.uio.no/pgp/`.

Die öffentlichen Schlüssel der Mitarbeiter und vieler anderer Personen erhalten Sie vom sogenannten Keyserver. Schreiben Sie dazu eine E-Mail mit dem Subject `help` an `pgp-public-keys@keys.pgp.net`. Die Schlüssel der Mitarbeiter finden Sie auch im WWW: Adresse `http://www.uni-muenster.de/URZ/Mitarbeiter/urzring.asc`.

Zur Kontrolle – und damit wir nicht mit Anrufen überschüttet werden – an dieser Stelle Daten der Schlüssel und die Fingerabdrücke:

```
Bits/KeyID  Date      Name/User ID
1024/3D37C6E1  1997/06/19  Dr. Klaus-Bolko Mertz <mertz@uni-muenster.de>
Key fingerprint = CA 6F 8D 5C EB 67 EA 18 38 79 64 3D 64 4C 4A 8C

1024/29A14DD1  1997/06/18  Reinhard Mersch <mersch@uni-muenster.de>
Key fingerprint = F0 AF 2B F1 FE 55 7A 3A E6 0D C7 27 29 50 22 26

1024/51F8EA05  1997/06/18  Mathias Grote <grote@uni-muenster.de>
Key fingerprint = 0F 13 5B 2D 1D A5 9D 65 DF EA 41 6B CE E5 88 C2

1024/BD7873F5  1997/06/17  Jürgen Hölters <holters@uni-muenster.de>
Key fingerprint = EA CB 47 AF 3A 79 96 B5 D3 46 C8 98 53 72 3F 2B

1024/44C661C5  1996/12/06  Stefan Ost <ost@uni-muenster.de>
Key fingerprint = 6F DB 21 B4 67 EA C2 E0 E8 3D 78 28 7C 66 09 38

1024/8A2097A5  1997/06/13  Rainer Perske <perske@uni-muenster.de>
Key fingerprint = AA D7 57 F5 8F 14 A7 A5 C4 E2 CF 04 95 52 25 60

768/D782E369   1997/07/18  Klaus Reichel <reichel@uni-muenster.de>
Key fingerprint = 6C 35 15 A9 E3 9E 83 4E 2E 95 4A F1 47 FC
```

Vor der Verwendung dieser Fingerprints sollten Sie natürlich überlegen, wie weit Sie dieser Quelle trauen dürfen ...

OpenGL – wenn Sie selbst Grafik programmieren wollen ...

E. Sturm

Früher wurde häufig GKS benutzt, wenn man selbst für die grafische Darstellung seiner Ergebnisse sorgen wollte. Diese Rolle könnte heute OpenGL einnehmen – und das sogar in 3D und als Animation.

OpenGL (*Open Graphic Language*) ist ein Software-Interface zu grafischer Hardware, im Grunde eine Sammlung von Unterprogrammen mit allem Drum und Dran. Ursprünglich entwickelt von der Fa. Silicon Graphics wird es auch auf anderen Plattformen unterstützt, z. B. auf vielen Unix-Systemen, auf OS/2, Windows 95/NT und Apple – unabhängig von der konkreten Hardware.

OpenGL deckt einen weiten Bereich der 2D- und 3D-Darstellung in Echtzeit ab, als da sind:

- Punkte, Linien und Polygone
- Beleuchtung und Transparenz
- Texturen
- Kantenglättung (*antialiasing*)
- atmosphärische Effekte
- Entfernung verdeckter Flächen
- Bewegungseffekte
- Doppelpufferung

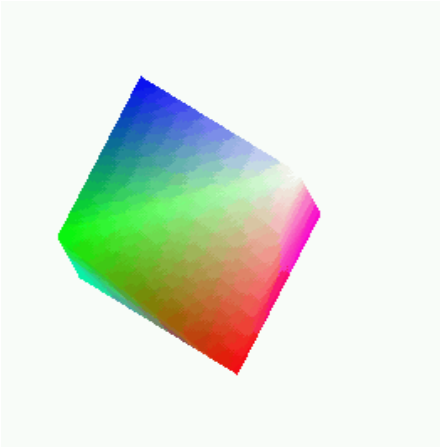

Abb. 1

Hinzu kommen Bibliotheken, die nicht-elementare Dinge ermöglichen wie z. B. die Erzeugung von NURBS (*Non-Uniform Rational B-Splines*). Außerdem gibt es jeweils Routinen zur Zusammenarbeit mit dem Betriebssystem: `glX` bei Unix-Systemen, `PGL` bei OS/2, `WGL` bei Microsoft-Systemen und `AGL` für den Apple Macintosh.

An Abb. 1 können Sie ermessen, wie leistungsfähig OpenGL ist. Das Oktaeder besitzt Flächen, die als Farbverlauf dargestellt sind. Auf einem Pentium 90 mit Matrox-Millennium-Grafikkarte dreht sich das Ganze dann noch – ruckfrei bis etwa zur Auflösung 300 × 300. Dabei werden nicht etwa fertige Bilder ausgetauscht, sondern jedes Pixel einzeln berechnet.

Informationen im WWW

Wer sich in OpenGL einarbeiten möchte, findet zunächst zwei Bücher:

- *OpenGL Programming Guide* – Second Edition, Addison Wesley, 1997
  ISBN 0-201-46138-2
- *OpenGL Reference Manual* – Second Edition, Addison Wesley, 1997
  ISBN 0-201-46140-4

Man beachte den Hinweis „Second Edition“! Die Beispiele zu diesen Büchern kann man sich im Internet abholen:

```
ftp://sgigate.sgi.com/pub/opengl/opengl1_1.tar.Z
```

Wie es heutzutage üblich ist, ist alles in C programmiert. Bis auf ein Beispiel (`tess.c`), wo es mit Arrays etwas durcheinander geht, kommt man aber mit Grundkenntnissen von C aus. (Ich persönlich ziehe es vor, C-Programme halbautomatisch nach PL/I zu übersetzen und dann weiter zu modifizieren.)

Auch eine Einführung kann man im WWW anschauen:

```
http://www.sgi.com/Technology/openGL/paper/opengl.html
```

Hinzu kommen noch jede Menge Seiten der beteiligten Firmen.

gl – glu – glut

Damit Sie eine Vorstellung davon erhalten, wie man bei der Bilderzeugung mit OpenGL vorgeht, seien hier ein paar Beispiele aufgeführt. Die Basissoftware `gl` ist für elementare Dinge zuständig. Will man z. B. ein rotes Dreieck darstellen, so schreibe man:

```
glBegin (GL_TRIANGLES);
glColor3f (1.0, 0.0, 0.0);
glVertex2f (5.0, 5.0);
glVertex2f (25.0, 5.0);
glVertex2f (5.0, 25.0);
glEnd();
```

Man spezifiziert den Typ des grafischen Elements (`GL_TRIANGLES`), seine Farbe (Rot, Grün, Blau) sowie Eckpunkte (engl. *vertex*). Üblicherweise beginnt der Name der Routine mit `gl` und endet mit Anzahl und Datentyp der Argumente (`f` steht für *float*).

Die Parameterlisten sind, wie man sieht, sehr kurz gehalten. Die Maxime von OpenGL ist: lieber mehr Aufrufe, dafür nur wenige Parameter. Damit das nicht auf Kosten der Effizienz geht, gibt es die Möglichkeit, sogenannte Display-Listen zu füllen, in denen die Befehle dann in „vorverdautem“ Format gespeichert werden.

Eine höhere Stufe stellen die `glu`-Routinen dar (*gl utilities*). Eine Kugel läßt sich z. B. erst mit einem `glu`-Aufruf erzeugen, der dann alles wieder in `gl`-Aufrufe (etwa für eine Display-Liste) zerlegt:

```
glusphere (QuadricObject,
  Radius,
  Längengrade,
  Breitengrade);
```

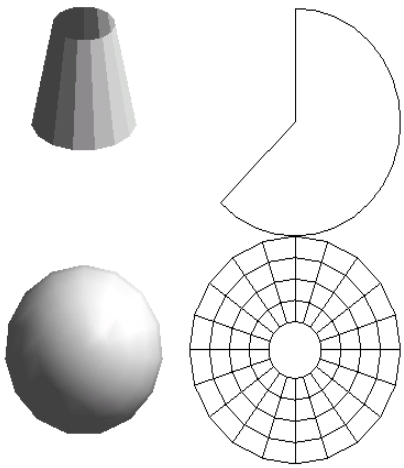

Abb. 2

Aber auch ein Polygon, das nicht konvex ist, muß zur Felderung (engl. *tesselation*) an eine `glu`-Routine übergeben werden, `gl` fühlt sich nur für konvexe Polygone zuständig. Ein Beispiel für die Möglichkeiten von `glu` zeigt Abb. 2.

Will man interaktiv und mit Animationen arbeiten, so muß man entweder die oben erwähnten Betriebssystemroutinen benutzen oder aber `glut` (*gl utility toolkit*). Mit `glut` steht einem eine betriebssystemunabhängige Fensterverwaltung zur Verfügung:

```
glutInitWindowSize (500, 500);
glutInitWindowPosition (100, 100);
glutCreateWindow ("Mein Fenster");
glutDisplayFunc (Display);
glutReshapeFunc (Reshape);
glutKeyboardFunc (Keyboard);
glutMainLoop();
```

Hiermit legt man fest, daß man ein Fenster öffnen möchte, und zwar der Größe 500 × 500 an der Position (100,100) mit dem Titelzeilentext „Mein Fenster“. Wenn das Fenster gezeigt werden soll, möge die eigene Routine `Display`, bei einer Veränderung der Fenstergröße die Routine `Reshape` und bei einer Tastatureingabe die Routine `Keyboard` aufgerufen werden. Bei `Keyboard` erfährt man z. B., welche Taste gedrückt wurde.

So richtig beeindruckend wird `glut` dann bei der Benutzung der oben erwähnten NURBS. In Abb. 3 sieht man eine Fläche, die im Grunde durch den Aufruf

```
gluNurbsSurface(theNurb,
    8, knots, 8, knots,
    4 * 3, 3, &ctlpoints[0][0][0],
    4, 4, GL_MAP2_VERTEX_3);
```

erzeugt wurde. Hier kommen dann doch ein paar Parameter mehr zusammen, was bei der Materie wohl unvermeidlich ist.

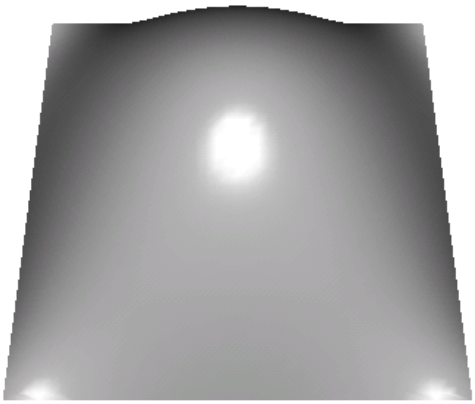

Abb. 3

Vom Bildschirm zum Drucker

Etwas Wichtiges habe ich bislang verschwiegen: OpenGL hat überhaupt nichts mit Druckern am Hut! Alles dreht sich nur darum, Pixelbilder auf dem Bildschirm zu erzeugen, und das möglichst effizient.

Es gibt allerdings drei Möglichkeiten, doch etwas zu Papier zu bringen. Entweder lesen wir das Pixelbild in eine eigene Variable und erzeugen uns daraus eine Bilddatei selbst, z. B. im P6-Format von `NetPBM` (das geht mit OpenGL- oder mit Betriebssystemmitteln). Oder wir gehen in den sogenannten Feedback-Modus und – erzeugen uns z. B. eine PostScript-Datei selbst.

Ich weiß gar nicht, warum Sie stöhnen – Sie wollten doch selbst programmieren! Aber – Spaß beiseite, es ist gar nicht so schwer! Die Bilder dieses Artikels sind der Beweis. Unser `plot`-Kommando „versteht“ sowohl P6- als auch PostScript-Dateien.

Sollten Sie Interesse an der Benutzung von OpenGL haben, so schreiben Sie mir bitte (`sturm@uni-muenster.de`). Das Rechenzentrum könnte dann z. B. entsprechende Programme zur Druckerunterstützung zur Verfügung stellen.

RUM-Lehre

Veranstaltungen in der vorlesungsfreien Zeit (September 1997)

Beratung zum Lehrangebot durch Herrn W. Bosse jeweils Di, Do 11-12, ✆ 83-31561

Im Herbst 1997 werden vom Universitätsrechenzentrum einige Veranstaltungen durchgeführt, die durch entsprechende Betreuung der Teilnehmer eigene Übungen fördern sollen. Das bedingt eine Begrenzung der Teilnehmerzahl. Interessenten werden deshalb gebeten, sich möglichst bald, spätestens jedoch eine Woche vor Beginn der entsprechenden Veranstaltung, im Dispatch des Universitätsrechenzentrums in die *Anmeldelisten* einzutragen, und sollten unbedingt zu dem angekündigten Beginn anwesend sein. Die entsprechenden Listen liegen bereits aus.

Wie in dem Artikel „Ausbildungsveranstaltungen zu Themen der DV“ dargelegt, können zu unserem Bedauern keine weiteren Veranstaltungen für das Wintersemester 1997/98 vom Universitätsrechenzentrum angeboten werden.

320178 Kommunikation und Information im Internet — Perske, R.
vom 15.9. bis 26.9.1997, ganztägig
Hörsaal: M2, Beginn: 15.9.1997, 11 Uhr

320182 Programmieren in Fortran 77 und Fortran 90 — Reichel, K.
vom 1.9. bis 12.9.1997, ganztägig
Hörsaal: Raum 107 Rechenzentrum, Beginn: 1.9.1997, 9 Uhr

320197 Statistische Datenanalyse mit dem Programmsystem SPSS — Nienhaus, R.
vom 15.9. bis 26.9.1997, ganztägig
Hörsaal: M4, Beginn: 15.9.1997, 9 Uhr

Kommentare zu den Lehrveranstaltungen

320178 Kommunikation und Information im Internet

In den letzten Jahren haben sich die internationalen Datenkommunikationsnetze, eines der wichtigsten ist das Internet, in rasantem Tempo ausgebreitet. Sie sind durch ihre Möglichkeiten zur Informationsgewinnung und zur Kommunikation ein unverzichtbares Hilfsmittel – nicht nur für Wissenschaftler.

Den Teilnehmern der Veranstaltung wird in praktischen Übungen gezeigt, wie man sich in dieser komplexen Welt zurechtfinden und sie sich zunutze machen kann. Vorausgesetzt werden nur elementare Kenntnisse im Umgang mit Computern.

Eine rechtzeitige vorherige Anmeldung im Dispatch des Universitätsrechenzentrums ist zur Teilnahme an den Übungen erforderlich.

Anmerkung: Das Universitätsrechenzentrum stellt für etliche Systeme, teilweise auch kostenlos, Software zur Verfügung, um die Möglichkeiten des Internets auch vom häuslichen Arbeitsplatz nutzen zu können. Die Mitarbeiter des DaWIN-Teams helfen Ihnen hier gerne weiter.

320182 Programmieren in Fortran 77 und Fortran 90

Fortran ist eine weitverbreitete Programmiersprache, die insbesondere für die Programmierung naturwissenschaftlicher und technischer Anwendungen eingesetzt wird.

In dieser Vorlesung sollen die Hörerinnen und Hörer lernen, wie Programme systematisch konstruiert werden. Gleichzeitig wird ihnen zunächst der Fortran-77-Standard, anschließend darauf aufbauend der neueste Fortran-90-Standard vermittelt. Es werden keine Programmierkenntnisse vorausgesetzt. Praktische Übungen sind Teil der Veranstaltung.

BRAUER: *Programmieren in Fortran 77*, Hüthig
MICHEL: *Fortran 90*, BI-Wiss.-Verlag
BRAINERD/GOLDBERG/ADAMS: *Fortran 90*, Oldenbourg
HEISTERKAMP: *Fortran 90*, BI-Wiss.-Verlag, University Press

320197 Statistische Datenanalyse mit dem Programmsystem SPSS

Das statistische Programmsystem SPSS (Statistical Package for the Social Sciences) wird in einer aktuellen Windows-Version vorgestellt und erprobt. Mit diesem System stehen bequem aufzurufende Programme zu den gebräuchlichen univariaten und multivariaten statistischen Verfahren sowie zur Datenaufbereitung zur Verfügung. SPSS wird z. B. zur statistischen Auswertung von Fragebögen eingesetzt.

In dieser Veranstaltung wird das programmtechnische Rüstzeug zur Durchführung derartiger Auswertungen vermittelt. Solide Grundkenntnisse bezüglich der anzusprechenden statistischen Verfahren sowie Kenntnisse der Anwendungsmöglichkeiten dieser Verfahren im jeweiligen Fachgebiet sind erwünscht und bei den praktischen Übungen von großem Nutzen.

SPSS GMBH: *SPSS für Windows, Anwenderhandbuch für das Basis System*
BÜHL/ZÖFEL: *SPSS für Windows Version 6*, Addison-Wesley
KÄHLER: *SPSS für Windows*, Vieweg

Liebe(r) Leser(in),

wenn Sie **infoWWW** regelmäßig beziehen wollen, bedienen Sie sich bitte des unten angefügten Abschnitts. Hat sich Ihre Adresse geändert oder sind Sie am weiteren Bezug von **infoWWW** nicht mehr interessiert, dann teilen Sie uns dies bitte auf dem vorbereiteten Abschnitt mit.

Bitte haben Sie Verständnis dafür, daß ein Versand außerhalb der Universität nur in begründeten Einzelfällen erfolgen kann.

Vielen Dank!

Redaktion **infoWWW**

An die
Redaktion **infoWWW**
Universitätsrechenzentrum
Einsteinstr. 60
48149 Münster

☐ Ich bitte um Aufnahme in den Verteiler.
☐ Bitte streichen Sie mich/den unten genannten Bezieher aus dem Verteiler.
☐ Meine Anschrift hat sich geändert.

Alte Anschrift:

_____

_____

Absender:

Name: _____

FB: _____ Institut: _____

Straße: _____

Außerhalb der Universität:

_____

(Bitte deutlich lesbar in Druckschrift ausfüllen!)

Ich bin damit einverstanden, daß die Angaben in der **infoWWW**-Leserdatei gespeichert werden (§ 4 DSG NW).

Ort, Datum

Unterschrift

H. P. fec.