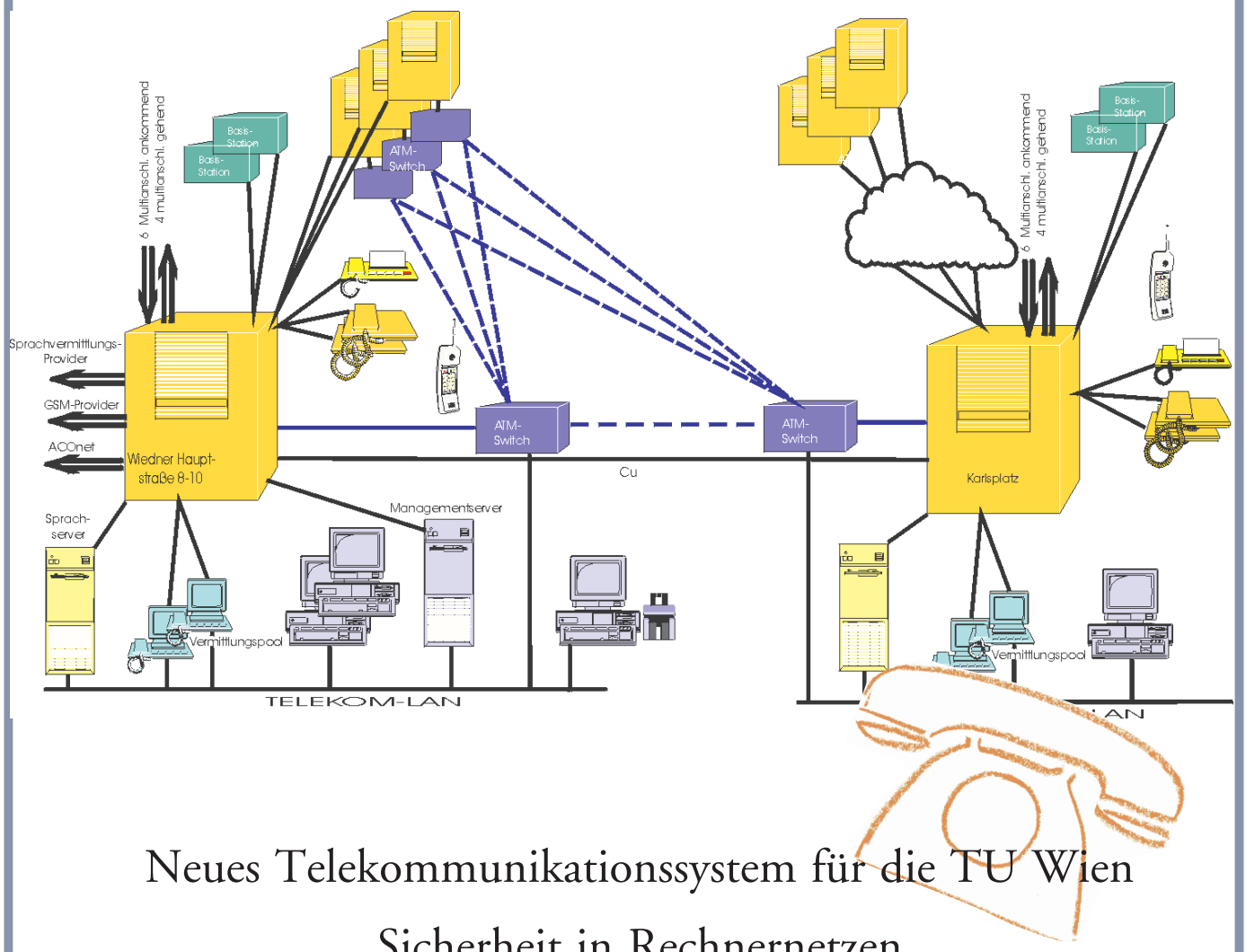
PIPELINE

INFORMATIONEN DES EDV-ZENTRUMS DER TECHNISCHEN UNIVERSITÄT WIEN



Neues Telekommunikationssystem für die TU Wien

Sicherheit in Rechnernetzen

NUMMER 25 JUNI 1998

Inhalt

Editorial

Liebe Leser!

Die TU Wien bekommt eine neue, moderne Telefonanlage. Lesen Sie dazu Details auf den ersten Seiten dieser PIPELINE.

Wir haben diesmal einen Schwerpunkt zum Thema Sicherheit in Rechnernetzen gesetzt. Zu diesem Zweck hat das EDV-Zentrum einen Experten vom Rechenzentrum der Humboldt-Universität zu Berlin zu einem Vortrag eingeladen und einige Artikel aus der dortigen Rechenzentrums-Zeitschrift zu diesem Thema mit freundlicher Genehmigung übernommen.

Seit Februar gibt es eine neu gestaltete Homepage des EDV-Zentrums und die WWW-Adresse wurde geändert. Verwenden Sie bitte in Zukunft als Einstiegsadresse `http://www.edvz.tuwien.ac.at/`.

Seit der Reorganisation im Jahre 1990 ist die Zeitschrift PIPELINE ein fester Bestandteil der Präsentation des EDV-Zentrums der TU Wien. Aufgrund der Tatsache, daß dies die Nummer 25 der PIPELINE ist, möchte ich speziell allen Kolleginnen und Kollegen am EDV-Zentrum sehr herzlich für die gute Zusammenarbeit danken: für ihre Bereitschaft, Berichte zu verfassen, obwohl sie keine Journalisten sind, und für jegliche technische Hilfe bei der Erstellung der einzelnen Hefte. Erfreulicherweise können wir auch stets die PIPELINE mit Beiträgen externer Autoren bereichern.

Ich freue mich auch, daß es immer gelungen ist, die Zeitung planmäßig fertigzustellen, daß die Zahl der Abonnenten trotz parallelem WWW-Angebot ständig steigt, und daß die PIPELINE auch außerhalb der TU Wien großes Interesse findet. Falls Sie Anregungen, Wünsche oder Beschwerden zur PIPELINE haben, wenden Sie sich bitte an die Redaktion. Mit dem nächsten Redaktionsschluß (14. September 1998) beginnen wir die nächsten 25 Hefte.

Irmgard Husinsky

Offenlegung gemäß § 25 Mediengesetz:

Herausgeber, Inhaber: EDV-Zentrum der Technischen Universität Wien

Grundlegende Richtung: Mitteilungen des EDV-Zentrums der Technischen Universität Wien

Redaktion: Irmgard Husinsky

Adresse: Technische Universität Wien, Wiedner Hauptstraße 8-10, A-1040 Wien
Tel.: (01) 58801-5484, 5481
Fax: (01) 587 42 11
E-Mail: husinsky@edvz.tuwien.ac.at
WWW: http://info.tuwien.ac.at/pipeline/

Druck: HTU Wirtschaftsbetriebe GmbH, 1040 Wien, Tel.: (01) 5863316

Das neue Telekommunikationssystem an der TU Wien

Endlich ist es soweit: die Technische Universität Wien erhält in den nächsten Monaten eine neue, dem modernsten Stand der Technik entsprechende Telefonanlage!

Derzeit wird die Telefonie an der Technischen Universität Wien noch mit 15 Nebenstellenanlagen – die zum Teil älter als 20 Jahre sind – betrieben. Die größte Anlage (Kapsch PKE 10000 im Freihaus) steht seit Jänner 1981 im Betrieb. Wie die jüngsten Ausfälle gezeigt haben, sind diese Anlagen zum größten Teil nicht mehr wartbar und entsprechen auch nicht mehr den Ansprüchen an die heutige Telekommunikation. So ist z. B. eine automatische Ausnutzung der jeweils günstigsten Tarife unterschiedlicher Provider (Least Cost Routing) prinzipiell nicht möglich. Deshalb hat die Universitätsdirektion bereits 1995 mit der Beauftragung eines Vorprojekts über eine neue Telekommunikationsanlage für die TU Wien die Initiative ergriffen. Am 24. 6. 1996 hat der Akademische Senat den Universitätsdirektor mit der Erstellung eines Konzepts für eine neue Telekommunikationsanlage betraut. In der Folge wurde Herr Ing. Wottawa von der Firma PKG-Data (inzwischen in DTN umbenannt) mit der Planung einer neuen Anlage beauftragt.

Nach Zustimmung des BMWV zum grundsätzlichen Konzept und zum detaillierten Pflichtenheft wurde Ende 1997 die EU-weite Ausschreibung der neuen Telekommunikationsanlage im *Supplement zum Amtsblatt der Europäischen Gemeinschaften* veröffentlicht. Am 11. März 1998 erfolgte die Anbotseröffnung. Am 30. April 1998 wurde die Post und Telekom Austria (als Generalunternehmer gemeinsam mit den Firmen Ericsson Austria AG und Mobilkom) mit dem in der Ausschreibung vorgesehenen Probebetrieb beauftragt. Der end- gültige Zuschlag soll im Juli 1998 erfolgen.

Das Gesamtprojekt, dessen Realisierung für 1998 und 1999 vorgesehen ist, gliedert sich in zwei Bauabschnitte: Im Herbst 1998 erfolgt die Umstellung der Hauptanlage und der kleineren Nebenstellenanlagen, im Sommer 1999 wird im Zuge der Inbetriebnahme des neuen Institutsgebäudes auch der Anlagenteil für die Favoritenstraße in Betrieb genommen.

Die technische Entwicklung in der Telekommunikation läßt die ursprünglich getrennten Bereiche der Sprach- und Datenkommunikation immer mehr zusammenwachsen. Das Konzept sieht daher die Nutzung eines gemeinsamen Backbones für Daten- und Telekommunikation vor. Deshalb wurde im Februar 1998 das EDV-Zentrum mit dem Betrieb der neuen Telekomanlage betraut.

Auszug aus dem Pflichtenheft (Allgemeine Beschreibung)

Für die Technische Universität Wien ist ein einheitliches, vollintegriertes, digitales Telekommunikationssystem aufzubauen, das die gesteckten Zielsetzungen:

- Einheitliche Kopfnummer für die TU Wien
- Sparen von Telefonkosten durch interne Vernetzung
- Senkung der Personalkosten durch zentralen Vermittlungspool
- Zentrale Wartung und Programmierung der Anlagen
- Kostentransparenz durch zentrale Auswertung der Gesprächsgebührendaten
- Kostentransparenz durch die klare Zuordnung jedes gebührenpflichtigen Gespräches
- Bessere Nutzung der Funktionalität von Telekommunikationsanlagen durch standortübergreifende Leistungsmerkmale (z.B. Anrufumleitung, automatischer Rückruf, Konferenzschaltung etc.)
- Senkung der Betriebskosten durch gemeinsame Nutzung der vorhandenen und neu zu schaffenden Infrastrukturen für Daten- und Telekommunikation
- Verbesserung der internen und externen Kommunikation durch den Einsatz von Sprachservern und Sprachspeichern
- Unterstützung von Multimedia-Applikationen – zukünftige ATM-Integration
- Corporate Network
- Errichtung einer Struktur für mobile Telekommunikation (DECT) als Option

mit einem einheitlichen, über die TU-Wien-Standorte verteilten und redundant aufgebauten Telekommunikationssystem umsetzt. Die Bedienung, die Leistungsmerkmale und die Anschlußmöglichkeiten an das Telekommunikationssystem müssen an allen Standorten gleich sein. Es ist damit eine einheitliche Funktionalität (Konfiguration von Team- und Chefsekretär-Anlagen, Nutzung von Leistungsmerkmalen etc.) ohne Einschränkungen über die örtlichen Standorte hinaus zu erreichen. Voraussetzung für eine wirtschaftliche, einheitliche Gesamtstruktur ist die Einbindung der Telekommunikationszentralen in den TUNET-Backbone. Aus Redundanzgründen sind die vorhandenen Kupferleitungen als zusätzlicher Leitungsweg zu nutzen.

Optional ist als Ergänzung zum Fest-Netz eine mobile Telekommunikationsvernetzung basierend auf dem DECT-Standard anzubieten.

Das neue Telefoniekonzept der TU Wien verfolgt mehrere Ziele: Zum einen sollen mit einem modernen digitalen Telekommunikationssystem im Endausbau (fast) alle Standorte der TU Wien einheitlich ausgestattet werden, sodaß die üblichen Funktionen eines Telefonsystems wie Vermittlung, Rufumleitung, automatischer Rückruf, Konferenzschaltung usw. auch standortübergreifend zur Verfügung stehen. Die TU Wien wird von außen an allen diesen Standorten über eine einheitliche Rufnummer erreichbar sein, wobei die Anrufe im internen Telekommunikationsnetz der TU auf die dezentralen, in den einzelnen Gebäuden installierten Subanlagen verteilt werden.

Zum anderen wird das neue Telefonsystem auch die erforderliche Kostentransparenz bieten und die Zuordnung der anfallenden Gesprächsgebühren auf die dafür vorgesehenen Kostenstellen (z. B. Dienstgespräche auf Institutsebene, aber auch auf ein Projektkonto oder ein persönliches Konto) ermöglichen, sodaß Maßnahmen zur Senkung der Telefonkosten auf dezentraler Ebene getroffen werden können. Durch Einbeziehung des TUNET Backbones und durch die Nutzung alternativer Leitungswege können weitere Einsparungen bei den laufenden Kosten erzielt werden. So wird die neue Anlage ein *Least Cost Routing* implementiert haben, d. h. es wird automatisch der Verbindungsaufbau durchgeführt, der zu den geringsten Gesprächsgebühren führt. Das gilt für alternative Festnetzbetreiber in- und außerhalb Österreichs oder für die ins Auge gefaßte Möglichkeit, für Gespräche mit anderen österreichischen Universitäten Übertragungskapazitäten des ACOnet zu nutzen. Grundsätzlich soll auch im neuen Telefonsystem die Fernwahlsperre beibehalten werden. Die bisherige Freigabe auf Wien wird auf Wien-Umgebung erweitert. Zusätzlich können aber alle Telefonapparate, von denen aus häufiger Ferngespräche geführt werden, mit einem Chipkartenleser ausgestattet werden. Mittels einer persönlichen Chipkarte, auf der die Kontonummer des betreffenden Gebührenkontos gespeichert ist, kann dann jeder Benutzer selbständig – ohne Inanspruchnahme der Vermittlung – seinen Telefonapparat für Ferngespräche freischalten und diese daher auch zu jenen Tageszeiten führen, wo die Telefonzentrale nicht mehr besetzt ist.

Digitale Sprachspeicherboxen können als persönlicher Anrufbeantworter genutzt werden, um Nachrichten zu hinterlegen und – auch von zu Hause – abzufragen. Der Sprachserver bietet aber auch die Möglichkeit, entsprechende Informationstexte für häufig nachgefragte Auskünfte unter eigenen Nebenstellennummern abzulegen.

Die neue Telekomanlage wird auch zur Verbesserung der Erreichbarkeit der Institute beitragen. Grundsätzlich sollen mit der neuen Telekomanlage alle Anrufe, die nicht entgegengenommen werden, nicht wie bisher sofort in die Telefonzentrale zurückfallen, da das Vermittlungspersonal in solchen Fällen nur selten eine Auskunft über die Erreichbarkeit des nicht angetroffenen Mitarbeiters geben kann. Solche Anrufe verbleiben vielmehr im betreffenden Institut und werden auf jene Nebenstellen umgeleitet, die vom Institut dafür ausgewählt werden (Institutssekretariat, Sprachspeicherbox etc.). Es bleibt der Institutsleitung überlassen, ob und von welcher Möglichkeit der Anlage Gebrauch gemacht wird und was mit solchen Anrufen jeweils geschehen soll – auch wenn es vermutlich nicht dem Selbstverständnis der Universität entspricht, wenn der erfolglose Anrufer aus dem Sprachspeicher sinngemäß die Auskunft erhält: „Ich bin derzeit nicht erreichbar und möchte auch künftig nicht gestört werden“. Die neue Telefonanlage bietet jedenfalls viele Möglichkeiten, die man nutzen kann, aber nicht muß.

Mit der neuen Telefonanlage werden auch alle Telefonapparate erneuert. Die neuen digitalen Endgeräte sind mit Funktionstasten für häufig benützte Nummern oder Funktionen sowie einem Display ausgestattet, auf dem Informationen (wer ruft mich an, wen rufe ich an, ...) angezeigt werden. Auf die optionale Ausstattung mit einem Chipkartenleser zur Aufhebung der Fernwahlsperre wurde bereits hingewiesen. Die Umstellung auf digitale Nebenstellen mag im einen oder anderen Fall zu Problemen führen, wenn die derzeitigen Geräte nicht mehr 1:1 umgestellt werden können. Anrufbeantworter können dann im allgemeinen nicht angeschlossen werden, aber die neuen Sprachspeicherboxen werden sie ohnehin ersetzen. Die bestehenden Fax-Geräte können im allgemeinen an Nebenstellen der neuen Telefonanlage angeschlossen werden und benötigen keine eigenen Amtsleitungen mehr (allerdings muß die Kennung umprogrammiert werden). In jedem Fall werden vor der Umstellung die mit der Installation des neuen Systems betraute Lieferfirma und das EDV-Zentrum gemeinsam mit den von den Instituten zu benennenden Kontaktpersonen die konkrete Vorgangsweise absprechen und einen detaillierten Klappen- und Geräteplan erstellen.

Der in der Ausschreibung vorgesehene Probebetrieb wurde auf das EDV-Zentrum und die Wirtschaftsabteilung beschränkt, um eine möglichst geringe Beeinträchtigung des normalen Betriebs unserer Universität zum Ende des Studienjahres sicherzustellen. Dieser Probebetrieb beginnt Anfang Juni. Im Probebetrieb wird auch DECT – Inhouse Mobilkommunikation – getestet. Die Mitarbeiter des EDV-Zentrums und der Wirtschaftsabteilung sind während des Probebetriebs natürlich weiterhin unter den gewohnten Nebenstellen zu erreichen.

Die Gespräche mit allen Instituten zur Festlegung der Geräteausstattung und der Nebenstellen sollen ab Mitte Juni bis Ende Juli stattfinden. Für das Wochenende 5./6. September – unmittelbar vor Schulbeginn – ist die Umschaltung der Hauptanlage der TU Wien vorgesehen. Danach werden die kleinen Anlagen schrittweise umgestellt. Für die Umstellung ist natürlich eine Information der Anrufer, die noch die alte Nebenstelle wählen, über einen Auskunftsserver vorgesehen.

Kontaktpersonen:

Dr. Johannes Demel:
Projektleitung am EDV-Zentrum
E-Mail: demel@edvz.tuwien.ac.at
Tel.: 01/58801 5829

Ing. Harald Wottawa:
Planungsfirma DTN
E-Mail: wottawa@ping.at
Tel.: 02252/49765

Dipl.-Ing. Friedrich Blöser:
Nummernplan, Betrieb der Telekomanlagen
E-Mail: bloeser@edvz.tuwien.ac.at
Tel.: 01/58801 5810

Johann Kainrath:
Gemeinsames Backbone Daten- und Telekommunikation, Verbindung mit den öffentlichen Netzen
E-Mail: kainrath@edvz.tuwien.ac.at
Tel.: 01/58801 5811

Dr. Manfred Siegl:
Verkabelung
E-Mail: siegl@edvz.tuwien.ac.at
Tel.: 01/58801 5604

Um die Institute rechtzeitig und umfassend über die neue Telekommunikationsanlage zu informieren, wird es eine Reihe von Informationskanälen geben:

- Im Juni finden Informationsveranstaltungen an mehreren Terminen für Vertreter der Institute zur Vorstellung der Eigenschaften der neuen Anlage und deren Apparate statt. Diese Veranstaltung dient auch zur Vorbereitung auf die Konfigurationsgespräche mit den Instituten.

- Einrichtung eines Demo-Raums (Seminarraum des EDV-Zentrums im Freihaus, 2.OG im Roten Bereich), in dem die neuen Endgeräte und die Anlagenfunktionen ausprobiert werden können.

- Direkte Information der Institute und Mitarbeiter.

- Online über WWW werden unter der Adresse http://www.edvz.tuwien.ac.at/telekom/ alle Informationen (aktueller Zeitplan und Termine, Hinweise zum Nummernplan und zur Konfiguration, Bedienungshinweise, Formulare, Gegenüberstellung der alten und neuen Nebenstellen, ...) zur Verfügung stehen.

Zeitplan:

2. Juni	Beginn Probebetrieb EDV-Zentrum, Wirtschaftsabteilung
10. Juni, 16.00	Informationsveranstaltung 1. Termin Freihaus HS 6
10. Juni	Inbetriebnahme des Vorführraums
17. Juni, 16.00	Informationsveranstaltung 2. Termin Freihaus HS 6
18. Juni	Beginn der Konfigurationsgespräche
29. Juni, 14.00	Informationsveranstaltung 3. Termin Freihaus HS 6
Ende Juli	Abschluß der Konfigurationsgespräche
Juli/August	Tausch aller Telefondosen
August	Anlieferung, Aufbau und Test der neuen Anlagen
5./6. September	Umschaltung der Hauptanlage auf die neue Telekommunikationsanlage
September	Benutzerschulung
Bis November	Umschaltung der weiteren Nebenstellenanlagen
Sommer 1999	Aufbau und Inbetriebnahme der Anlage in der Favoritenstraße

Da das neue Telekommunikationssystem der TU Wien für die Versorgung der gesamten Universität konzipiert ist, müssen für alle Telefonanschlüsse neue, fünfstellige Nebenstellen vergeben werden. Diese werden nicht wie bisher gebäude- sondern institutsbezogen sein (die ersten drei Stellen sind dann die Institutsnummer). Die Hauptnummer der TU Wien bleibt weiterhin 58801. Es ist völlig klar, daß die flächendeckende Umstellung des Rufnummernplans eine organisatorische Herausforderung erster Ordnung darstellt, zumal diese Umstellung gleichzeitig für das gesamte System erfolgen muß. Das EDV-Zentrum ist jedoch zuversichtlich, mit Unterstützung der mit der Installation des neuen Systems betrauten Lieferfirma und der beauftragten Firma DTN auch diese organisatorische Hürde halbwegs erfolgreich zu bewältigen. Zweifellos wird es aber auch Pannen und „Kinderkrankheiten“ mit dem neuen System geben, für die wir bereits jetzt um Nachsicht ersuchen.

Johannes Demel, Wolfgang Kleinert

Online-Zugang über TeleWeb

TeleWeb Internet-Zugang

Die Technische Universität Wien und die Firma Telekabel Wien Ges.m.b.H. bieten gemeinsam TU-Angehörigen (Studierenden, die eine Berechtigung für das Mail/News/Info-Service haben, und Mitarbeitern im Personalstand der TU Wien) als Alternative zum kostenlosen Internet-Zugang über die Universität einen Internet-Zugang via TeleWeb an.

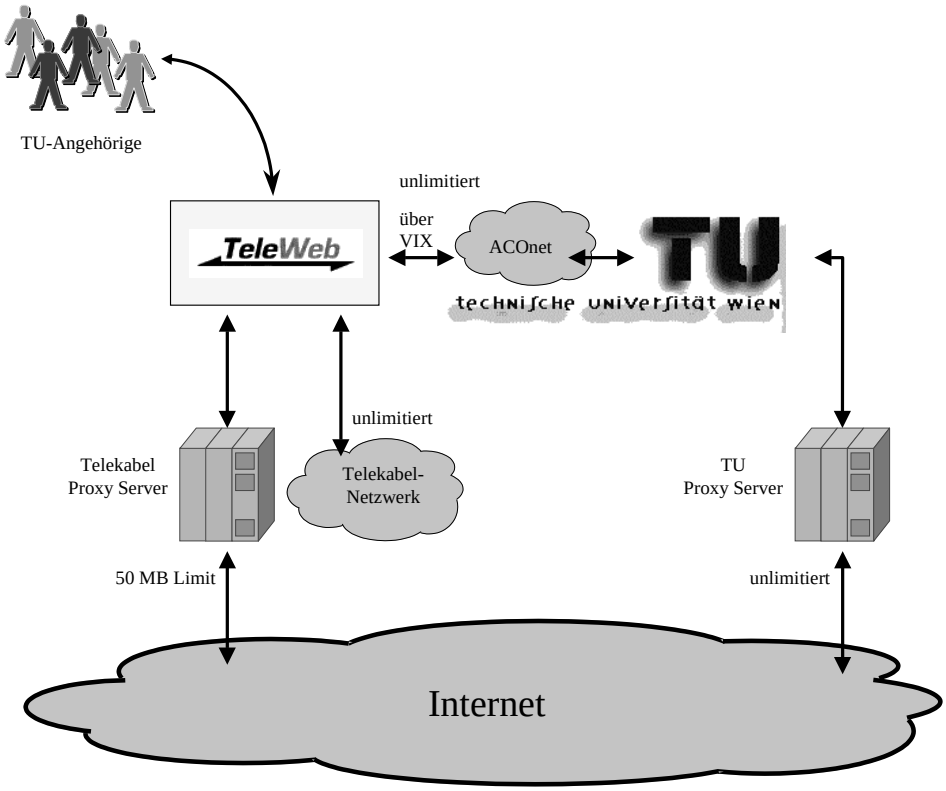
Dieser TeleWeb Dienst ermöglicht über ein Kabelmodem und die Fernsehsteckdose, über die der Computer mit dem Telekabel-Netzwerk verbunden ist, einen 24 Stunden Online-Zugang zum Internet (unabhängig vom Telefonanschluß). Beim TeleWeb Paket handelt es sich um ein modifiziertes TeleWeb Privatpaket zu einem Fixpreis von ATS 390,- pro Monat (gegenüber ATS 590,-). Dieses Angebot gilt nur für Studierende und Mitarbeiter im Personalstand der TU Wien mit einem aktiven Telekabel-Anschluß in interaktiv ausgebauten Gebieten der Telekabel.

Neben dem zeitlich unbegrenzten Zugang (die Verrechnung erfolgt über eine monatliche Gebühr und nicht nach der Zeit, die der Netzzugang genutzt wurde) ist auch mengenmäßig beim Zugang ins Internet über den TU Proxy kein Limit vorhanden. Während also das Surfen über den TU Proxy unlimitiert ist, besteht beim Zugang über den TeleWeb Proxy eine Beschränkung beim Datenvolumen aus dem / in das Internet von 50 MB pro Monat.

- **Datenvolumen aus dem / in das Internet**

Zugang zum ACOnet über VIX	unlimitiert
Zugang zum Internet über den Proxy der TU Wien für TeleWeb Paket	unlimitiert
Zugang zum Telekabel Netzwerk	unlimitiert
Zugang zum Internet über den Proxy der Fa. Telekabel	50MB/Monat

Telekabel vergibt in diesem Paket keine Mailadresse, sondern der Mail-Verkehr ist weiterhin mit der TU Mailadresse über den Account auf einem TU Mailserver abzuwickeln. Der Zugriff auf den News-Server der TU Wien ist für diese TeleWeb Teilnehmer erlaubt.



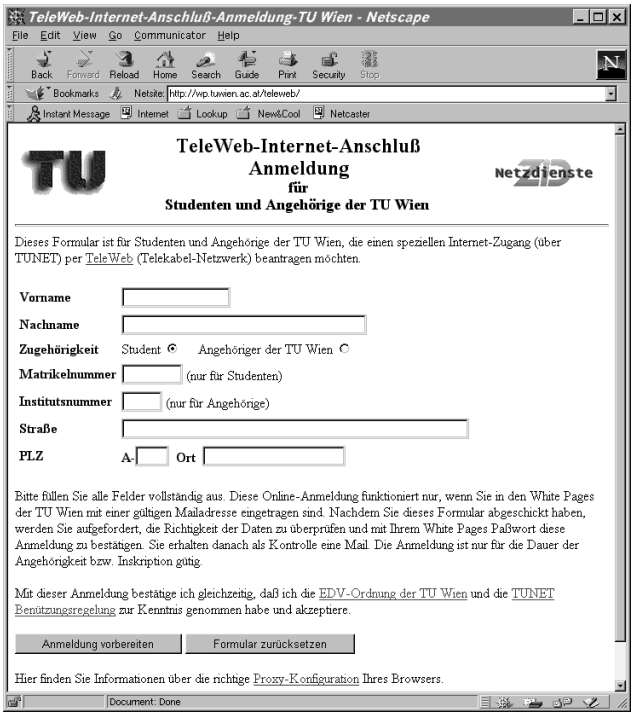
- **Kosten**

Der monatliche Preis für den TeleWeb Internet-Zugang beträgt ATS 390.-. Dazu kommt noch eine entsprechende Anschlußgebühr. Die genauen Beträge entnimmt man am besten diversen Tarifblättern der Firma Telekabel, die unter `http://www.teleweb.at` zu finden sind.

- **Anmeldeformalitäten**

Wenn sich ein TU-Angehöriger oder ein Student für das TeleWeb Angebot interessiert, kann er sich dazu online auf einer WWW-Seite der TU mit seinen Benutzerdaten anmelden. Die Online-Anmeldung über die WWW-Seite der TU funktioniert nur, wenn eine Eintragung in den White Pages der TU Wien mit einer gültigen Mailadresse und einem persönlichen Passwort existiert (TU-Angehörige sollten sich an ihren Address-Manager wenden, falls diese Voraussetzungen nicht zur Gänze erfüllt sind). Nach erfolgreicher Online-Anmeldung und Erhalt einer Bestätigungs-Mail hat der Benutzer bei der Fa. Telekabel die restlichen Formalitäten zu erledigen (Unterzeichnung eines Vertrages des Benutzers mit Telekabel).

Die Einstiegsseite ist unter `http://wp.tuwien.ac.at/teleweb/` zu erreichen, wo auch alle TUNET relevanten Informationen bez. Benützungsregelung und Konfiguration (Proxy-Einstellungen) verfügbar sind.



- **Wann läuft der TeleWeb Zugang ab ?**

Verliert ein Student oder Angehöriger der TU Wien seinen Eintrag in den White Pages, erlischt damit auch automatisch die TeleWeb Berechtigung. Sollte es aus besonderen Umständen (z. B. Namensänderung durch Heirat) fälschlicherweise zu so einer Situation kommen, wenden Sie sich bitte rechtzeitig an das EDV-Zentrum, um diesem Fall vorzubeugen.

- **Allgemeine Hinweise und Informationen**

Im Rahmen des TeleWeb Zuganges gelten die EDV-Ordnung der TU Wien und die TUNET Benützungsregelung sowie die entsprechenden TeleWeb Geschäftsbedingungen und Anschlußvereinbarungen. Bei Problemen mit Ihrem Telekabelanschluß bzw. mit Fragen zur PC-Konfiguration wenden Sie sich an den Telekabel HelpDesk unter der Telefonnummer 1701-33 oder via E-Mail an `help@telekabel.at`

Aktuelle Informationen über TeleWeb Zugang unter `http://www.teleweb.at/student/`

Johann Kainrath, Martin Rathmayer

TU Proxy – Browser Konfiguration

Am Proxy-Server der TU Wien `proxy.tuwien.ac.at` ist für diesen Internet-Zugang ein SOCKS-Server auf Port1080 installiert.

Für die Browser Netscape Communicator und Microsoft Internet Explorer kann folgende Einstellung verwendet werden:

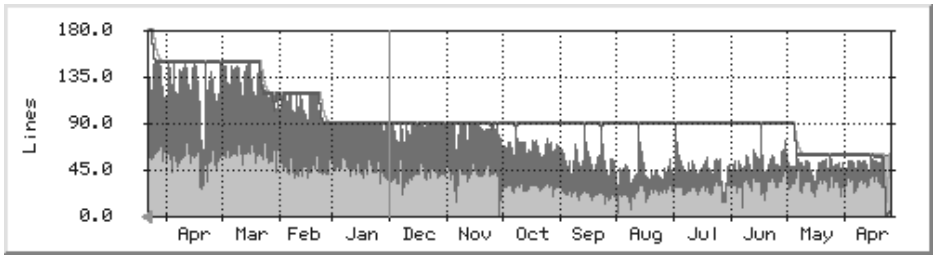
Netscape Communicator:
Edit | Preferences | Advanced | Proxies
Automatic proxy configuration
Configuration location (URL):
`http://proxy.tuwien.ac.at/tu.teleweb`

Microsoft Internet Explorer:
View | Internet Options | Connection | Configure
Automatic Configuration
URL: `http://proxy.tuwien.ac.at/tu.teleweb`

Mit dieser Konfiguration sind Hosts im Bereich `*.teleweb.at` und `*.ac.at` direkt über das TeleWeb-Netzwerk erreichbar, für alle anderen Hosts im Internet wird der Proxy-Server der TU Wien verwendet.

Ausbau des Wählleitungszuganges

Im März dieses Jahres wurde der Wählleitungszugang zur TU Wien auf 150 Leitungen erweitert. Im Zuge des kontinuierlichen Ausbauplanes wurde die notwendig gewordene Aufstockung um weitere 30 Kanäle (ein Multi-ISDN-Anschluß [PRI = Primary Rate Interface] mit 30 B-Kanälen und einem D-Kanal, das entspricht einer 2Mbit/s Strecke) am 7. Mai 1998 vorgenommen (siehe Abbildung aus TUNET Verkehrsstatistiken unten). Es stehen also derzeit insgesamt **180 gleichzeitige Zugänge** sowohl über analoge Modems als auch über ISDN den Angehörigen der TU Wien und Studenten zur Verfügung. Von der technischen Seite her bleibt der Zugang unverändert. Unter der bekannten Online-Tarif-Nummer **07189 15893** ist analog der Zugang bis zu 56kBit/s Geschwindigkeit mittels K56flex Standard und auf ISDN-Seite synchronous PPP über ISDN (HDLC ISDN) mit PAP Validierung möglich.



"Yearly" Graph (1 Day Average)

```
Max Use:  180.0 B/s (100.0%) Average Use:  36.0 B/s (20.0%) Current Use:   63.0 B/s (35.0%)
Max Line: 180.0 B/s (100.0%) Average Line: 97.0 B/s (53.9%) Current Line: 179.0 B/s (99.4%
```

V.90 ist die offizielle Bezeichnung der ITU Entwurfsempfehlung für 56K Modems. Derzeit ist V.90 noch nicht der offizielle 56K Modem-Standard, dies wird er erst nach Zustimmung aller ITU Mitglieder voraussichtlich im September 1998. Einiges der Lucent K56flex Technologie wird in V.90 enthalten sein (genauere Informationen siehe `http://www.k56flex.com/whatv90.html`).

Nach Informationen der Herstellerfirma Cisco ist auf unseren Terminalservern die Unterstützung von V.90 für das 2./3. Quartal 1998 angekündigt. Sobald eine stabile Version verfügbar ist, wird diese im Dialin-Service der TU Wien eingesetzt.

Aus technischen und organisatorischen Gründen ist eine Änderung des IP-Adressbereiches für den Wählleitungszugang erforderlich. Es erfolgt die Übersiedlung in ein Class C Netz (192.35.243.0 mit Maske 255.255.255.0). Für Sie als Benutzer sollte dadurch im Regelfall keinerlei Änderung in der Konfiguration Ihrer Dialin-Software notwendig sein. Die Umstellung findet im Rahmen des Netzwartungstages am Montag, dem 8. Juni 1998 statt.

Johann Kainrath

Ausbau der TUNET Institutsversorgung

Auch heuer wieder werden Ausbauarbeiten von TUNET im Access-Bereich durchgeführt. So wie in den vergangenen Jahren auch, wird eine strukturierte Verkabelung gemäß der Norm EN50173 hergestellt. Es werden Etagenverteiler errichtet, und Twisted-Pair Kabel installiert.

Die Planung zur Erstellung einer EU-weiten Ausschreibung wird durch die Firma DTN, Ing. Wottawa, durchgeführt.

Es ist vorgesehen in folgenden Bereichen Installationen durchzuführen:

Aspanggründe:	Neue TransAlpina Halle
Karlsplatz:	AD/AAEG, AF01
Getreidemarkt:	BA03, BD03, BEEG-06
Gußhausstraße:	CA01, CA03, CB01, CC01, FA02, FB01-04
Freihaus:	DA/DBEG, DA04, DA07, DA08, DB03, DB05, DB06, DB07, DB08

Die Durchführung der Arbeiten erfolgt vermutlich in der Zeit von September bis November 1998.

Bei den aktiven Netzkomponenten ist vorgesehen, nur noch Switches zu beschaffen. Insbesondere sollen teilweise auch Thinwire-Repeater durch Switches ersetzt werden, sodaß zumindest jedes Institut eine eigene Collission Domain erhält und keine Endsysteme mehr an Thickwire-Backbones direkt angeschlossen sein werden. Durch diese Maßnahme wird die Sicherheit in TUNET ein wenig gesteigert.

Manfred Siegl

Sicherheit in Rechnernetzen

Die Tatsache, daß in den letzten Monaten leider einige erfolgreiche Attacken auf Linux- und Windows NT-Systeme an der TU Wien stattgefunden haben, haben wir zum Anlaß genommen, einen Schwerpunkt zu diesem Thema zu setzen. Das EDV-Zentrum hat zu diesem Zweck einen kompetenten Vortragenden eingeladen. Alexander Geschonneck ist Sicherheitsbeauftragter am Rechenzentrum der Humboldt-Universität zu Berlin und Mitarbeiter des DFN-Projektes (Verein zur Förderung eines Deutschen Forschungsnetzes) „Firewall – ein Kernstück zur Sicherung des Verwaltungsnetzes der Humboldt-Universität". Er ist auch als Sicherheitsberater und Gutachter für Industrieunternehmen und in verschiedenen Netzwerksicherheitsgremien tätig.

Am 14. Mai hielt Herr Geschonneck einen Vortrag am EDV-Zentrum über Firewall-Systeme, beschrieb die Einrichtungen und Sicherheitsmaßnahmen an seiner Universität und stand zur Diskussion zur Verfügung. Für 15. Mai wurden die uns bekannten Systemadministratoren an den Instituten der TU Wien zu einer Informationsveranstaltung eingeladen. In seinem Vortrag vor etwa 70 Personen gab Herr Geschonneck einen Überblick über die verschiedenen Arten möglicher Systemeinbrüche über das Netz, zeigte Fehler auf, die bei Netzkonzeption, Administration, Implementation und Anwendungen vermieden werden sollten, und präsentierte Lösungsvorschläge zur besseren Sicherung von Rechnernetzen. Die Vortragsfolien sind unter http://www.edvz.tuwien.ac.at/security/ zu finden.

Das Rechenzentrum der Humboldt-Universität zu Berlin gestaltete im Dezember 1997 eine Ausgabe ihrer RZ-Mitteilungen ausschließlich zum Thema Sicherheit in Rechnernetzen (siehe http://www.hu-berlin.de/inside/rz/rzmit/rzmit.html). Aus diesem Heft drucken wir mit freundlicher Genehmigung der Autoren und der Redaktion vier Artikel ab.

„Der Tag danach ..." gibt Empfehlungen, was man nach einem erfolgten Einbruch tun kann. „SSH – dem Lauscher keine Chance" beschreibt den Einsatz und die Installation von Secure Shell (SSH), das eine verschlüsselte Telnet-Verbindung ermöglicht. Dieses Programm ist für alle gängigen Plattformen als Campuslizenz an der TU Wien verfügbar und wird vom EDV-Zentrum empfohlen. „Internet-Sicherheit von Windows-Rechnern" zählt Schutzmöglichkeiten unter Windows NT auf. „Sicherheitsrisiken mit aktiven Webseiten" beschäftigt sich mit Java, JavaScript und Cookies unter dem Aspekt der Sicherheit.

Schließlich soll noch darauf hingewiesen werden, wie wichtig ein verantwortungsvoller Umgang mit Paßwörtern von Benutzeraccounts im Interesse aller Teilnehmer in einem Netz ist. Wählen Sie ein sicheres Paßwort, ändern Sie es häufig und geben Sie es nicht an andere Personen weiter (siehe z.B. auch http://www.hu-berlin.de/rz/rzmit/rzm12/rzm12_18.html).

Wolfgang Kleinert

Der Tag danach ...

Die Vorstellung, daß ein System hundertprozentig sicher sei, ist oft ein Trugschluß. Hier soll kurz darauf eingegangen werden, was zu tun ist, wenn ein Einbruch auf einem UNIX-System festgestellt wurde. Auch wenn Ihr UNIX-System nicht kompromittiert wurde, helfen vielleicht diese Hinweise, Ihr System richtig abzusichern. Die Erfahrung zeigt, daß es kein Patentrezept für die Reihenfolge der Maßnahmen gibt. Sie richtet sich in der Regel nach der Schwere des Angriffs, den eigenen Fähigkeiten und den zur Verfügung stehenden Ressourcen.

Es erscheint immer ratsam, vom kompromittierten System ein Komplettbackup anzulegen. Dies kann helfen, falls man bei der Suche Spuren und Daten zerstört.

1. Versuchen Sie, die Spur des Eindringlings zu seinem Ausgangspunkt zurückzuverfolgen. Dazu sollten Informationen aus folgenden Quellen zu Rate gezogen werden:

- `who`
- `w`
- `last`
- `lastcomm`
- `netstat`
- `snmpnetstat`
- Informationen des Routers
- `/var/adm/messages` etc. – Eindringlinge versuchen häufig, Mails an „ihre" Accounts zu schicken
- `syslog` – schickt Syslogmeldungen an einen eventuell vorhandenen Loghost
- Logfiles von `tcp_wrapper`, `cgi_wrapper`, `suid_wrapper` und ähnlicher Software
- `finger` auf alle lokalen Nutzer; Informationen, wer sich wann von wo aus als Letzter angemeldet hat, können von großem Nutzen sein
- History-Dateien von Shells, `.history` etc.
- Mailboxen kompromittierter Accounts.

Informationen der Befehle `who`, `w`, `last` und `lastcomm` basieren in der Regel auf `/var/adm/pacct`, `/usr/adm/wtmp`, `/etc/utmp` etc. Die meisten Hintertürprogramme von Eindringlingen verhindern aber das Speichern von Informationen in diesen Dateien. Wenn ein Eindringling noch nicht dazu gekommen ist, diese Hintertürprogramme zu installieren oder die Dateien einfach zu löschen, kann man dort eventuell Informationen finden. Dies trifft besonders zu, wenn Sie keine

Standardnamen oder Verzeichnisse für diese Dateien definiert haben.

Hilfreich ist die Installation von `xinetd` oder `tcp_wrapper`. Mit diesen Tools kann man u. a. alle Verbindungsversuche frühzeitig protokollieren, noch bevor der angesprochene Daemon via `inetd` gestartet wird. Sinnvoll ist auch ein Weiterleiten von `Syslog`-Informationen zu einem zentralen, speziell abgesicherten Loghost mit semi-automatischer Intruder Detection. Es gibt eine Vielzahl von Intruder Detection Systemen, die im Netzverkehr nach speziellen Hackersignaturen suchen und entsprechende Maßnahmen einleiten. Auch eine simple Protokollierung der Verbindungsanforderungen im lokalen Netzwerk hilft oft, Einstiegslöcher zu orten.

2. Schließen Sie alle externen Netzzugänge zu diesem System. Dies kann durch Beenden der lokalen Netzwerkdienste oder durch eine physische Trennung vom Netzwerk geschehen. Ein sich entdeckt geglaubter Eindringling könnte sonst versuchen, seine Spuren zu verwischen, beispielsweise mit `rm -rf /`. So kann sich ein „nur Neugieriger“ schnell in einen Vandalen verwandeln.

3. Vergleichen Sie die auf dem System vorhandenen Programme mit den Originaldateien des Herstellers oder der Originaldistribution. Achten Sie besonders auf folgende Programme, da sie häufig durch trojanische Pferde ersetzt werden, die dem Eindringling eine vom Administrator unbemerkte Hintertür öffnen:

- `/bin/login`
- `/usr/etc/in.*` (z. B. `in.telnetd`)
- `/lib/libc.so*`
- alle Programme, die von `inetd` gestartet werden (in `/etc/inetd.conf` definiert).

Häufig werden auch folgende Programme ersetzt:

- `netstat` – Netzverbindungen können „versteckt“ werden
- `ps` – laufende Prozesse können „versteckt“ werden (z. B. ein Paßwort-Crackprogramm)
- `ls` – Verzeichnisse oder Dateien können „versteckt“ werden
- `ifconfig` – verschleiert, daß sich ein Netzwerkdevice im Promiscuous Mode befindet und so den gesamten Netzwerkverkehr ablauscht
- `sum` – Prüfsummen der Originalprogramme werden verfälscht wiedergegeben; meistens werden aber die Programme so verändert, daß sie die Originalprüfsummen aufweisen(!).

Mit `ls -lac` kann man den Zeitpunkt der Veränderung von Dateien überprüfen. Überprüfen Sie alle Ihnen zur Verfügung stehenden Protokolldateien auf Hinweise, daß die Systemzeit verändert wurde. Vergleichen Sie Dateigröße und MD5-Prüfsummen mit den Daten auf den Original-Installationsmedien oder den MD5-Prüfsummen, die Sie nach der Installation erstellt haben. Sie haben doch MD5-Prüfsummen erstellt, oder?

Eine andere populäre Hintertür ist das Hinzufügen des `suid`-Bits zu einem normalen Programm (z.B. `/bin/time`), um dieses von einem normalen Account mit Administratorrechten auszuführen. Sie können alle vorhandenen `suid`-Programme mit `find / -type f -perm -4000 -exec ls -la` ausfindig machen.

Das unbedingt zu empfehlende Programm `tripwire` überwacht die Veränderung von Systemdateien und -verzeichnissen. Bei Unsicherheiten, ob noch Hintertürprogramme vorhanden sind, sollte das gesamte System neu installiert werden.

4. Installieren Sie Mechanismen, die sicherstellen, daß die Nutzer ihr Paßwort regelmäßig erneuern. Mit `anlpasswd, npasswd` oder `passwd+` können Sie Programme einsetzen, die als Ersatz für `/bin/passwd` oder `/bin/yppasswd` die Nutzer dazu zwingen, sichere Paßwörter zu wählen. Dieses geschieht zum einen durch einen einfachen Rulecheck und zum anderen durch Wörterbuchabfragen. Setzen Sie selbst Paßwort-Rateprogramme wie Crack ein und überprüfen Sie, ob die Nutzer sichere Paßwörter gewählt haben, bevor es der Eindringling für Sie tut. Sinnvoll ist auch der Einsatz von Einmalpaßwortsystemen, wie z. B. S/Key oder OPIE.

5. Überprüfen Sie die Dateien `.rhosts` und `.forward` in jedem Nutzerverzeichnis (besonders auch Administrator- und Systemaccounts) nach verdächtigen Einträgen. Enthält z. B. die Datei `/.rhosts` den Eintrag `+ +`, bedeutet das, daß sich jeder Nutzer von jedem anderen System im Netzwerk als Administrator ohne Paßwortabfrage anmelden kann. Das Programm `COPS` beinhaltet u. a. ein Script, mit dem solche verdächtigen Einträge aufgespürt werden.

Mit `find / -name .rhosts -exec ls -o -name .forward` kann man dies auch selbst tun (evtl. per Cronjob).

Suchen Sie nach allen Dateien, die in der Zeit erstellt oder verändert wurden, die als Angriffszeit vermutet wird, mit `find / -ctime -2 -ctime +1 -exec ls`.

Alle Dateien `.login, .logout, .profile, .cshrc, .bashrc, .bash_profile` in den Nutzerverzeichnissen sollten nach verdächtigen Einträgen und der Uhrzeit überprüft werden. Stellen Sie sicher, daß die Verzeichnisse von gesperrten oder System Accounts (sync, news, sundiag) keine `.rhosts`-Datei enthalten. Diese Accounts sollten als Login-Shell `/bin/false` haben. Suchen Sie in allen Verzeichnissen nach Dateien, die mit „`.`“ oder „`..`“ beginnen. Diese werden häufig in `/tmp, /var/tmp, /usr/spool/*` oder in anderen für Nutzer schreibbaren Systemverzeichnissen gefunden. Es kommt auch vor, daß Dateien versteckt werden, die Zeichen wie `^T` etc. im Dateinamen enthalten oder mit „`...`“ oder „`..` “ (Punkt, Punkt, Leerzeichen) beginnen. Dies soll eine Inspektion erschweren.

6. Prüfen Sie, daß Ihre mit NFS exportierten Verzeichnisse nicht für jeden schreibbar sind. Mit `showmount -e` können Sie überprüfen, welche Filesysteme Sie mit welchen Rechten exportieren. Einige ältere NFS-Server ignorieren Access-Listen, wenn sie eine bestimmte Größe

überschreiten. Kontrollieren Sie, was Sie wie importieren! Wenn möglich sollte das `nosuid`-Flag gesetzt sein.

7. Stellen Sie unbedingt sicher, daß Sie die aktuellste `Sendmail`-Version installiert haben oder installieren Sie einen `Sendmail_wrapper`.

8. Versuchen Sie, alle Security-Patches zu installieren, die der Hersteller Ihres Systems veröffentlicht hat. Beziehen Sie diese Patches nur von einer vertrauenswürdigen Stelle und überprüfen Sie gegebenenfalls die digitalen Signaturen.

9. Informieren Sie alle befreundeten Sites und Systeme, daß Ihr System kompromittiert wurde. Vertrauen ist häufig symmetrisch. Wenn Sie einem System via `.rhosts` oder `/etc/hosts.equiv` trauen, wird es Ihnen wahrscheinlich auch trauen. Ein Eindringling kann sich so von System zu System „durchhangeln“, weltweit. Es ist dringend ratsam, eine geeignete zentrale Koordinierungsstelle für Netzwerksicherheit zu informieren (z.B. DFN-CERT).

10. Installieren Sie einen Packet-Filter oder ein Firewall-System am Übergang zu Ihrem Internet Service Provider.

Eine kurze unvollständige Checkliste, um den Sicherheitsstatus zu überprüfen:

- Mit `rpcinfo -p` können Sie auf Ihrem System überprüfen, ob RPC-Dienste laufen, die eigentlich nicht laufen sollten, z.B. `rexd`.
- Prüfen Sie `/etc/hosts.equiv` auf den Eintrag `+`.
- Prüfen Sie, ob `tftp` auf Ihrem System deaktiviert ist. Wenn es unbedingt laufen muß, dann stellen Sie sicher, daß es nicht mit Superuserprivilegien läuft und es mit der Option '`-s`' auf einen sicheren Bereich zeigend gestartet wird. Setzen Sie den `tcp_wrapper` ein und beschränken Sie den Zugriff.
- `cron`- und `at`-Jobs sollten auf „Zeitbomben“ überprüft werden.
- Überprüfen Sie die Scripte, die beim Systemstart abgearbeitet werden (`/etc/rc.boot, /etc/rc.local` oder bei SYSV `/etc/rc*.d/*`). Prüfen Sie alle anderen Dateien in `/etc/`, die Systemkonfigurationen enthalten (`sendmail.cf, hosts.allow, at.allow, at.deny, cron.allow, hosts, hosts.lpd` etc.). Die Datei `/etc/aliases` sollte keine Definition verdächtiger Accounts beinhalten (`uudecode` ist nur ein Beispiel).
- Die Datei `/etc/inetd.conf` sollte keinen Dienst enthalten, der eventuell vom Eindringling hinzugefügt wurde.
- Kopieren Sie alle Logdateien an einen sicheren Ort, damit Sie sie später kontrollieren können. Sie könnten unangenehm überrascht werden, wenn der Eindringling nur vergessen hat, sie zu löschen und es später nachholt. Suchen Sie nach anderen temporären Dateien, die eventuell während des Angriffes erstellt worden sind und Hinweise auf das Vorgehen des Eindringlings geben. (Werfen Sie dazu einen Blick auf `/tmp`, bevor Sie rebooten.)
- Legen Sie eine Sicherungskopie von `/etc/passwd` an und verwahren Sie sie auf einem anderen sicheren System. Ändern Sie die Paßwörter der privilegierten Nutzer, wenn Sie sicher gestellt haben, daß `/bin/passwd` und `/bin/su` nicht kompromittiert wurden. Alle Nutzer müssen ihr Paßwort umgehend ändern, denn es könnte sein, daß der Eindringling bereits Paßwörter erraten hat. Sperren Sie gegebenfalls alle Accounts.
- Prüfen Sie, ob die vorhandenen Dienste ordnungsgemäß konfiguriert sind (Anon-FTP, WWW etc.).
- Installieren Sie Wrapper- und Audit-Software.
- Definieren Sie nur `/dev/console` als sicheres Terminal, so daß sich der Superuser nicht über das Netz anmelden darf.
- Überprüfen Sie `/etc/hosts.equiv, /etc/hosts` und `.rhosts` auf Einträge wie # u. ä. Der Eindringling kann durch Fälschung von DNS-Informationen als Host # auftreten. Er würde dann als vertrauenswürdig eingestuft und hätte Zugang zu Ihrem System. Diese Dateien werden gern vom Hersteller mit `# comment` ausgeliefert.
- Es gibt sehr viele Mittel und Wege, in ein System einzudringen.

Halten Sie die Augen immer offen!

Diesen Artikel haben wir mit freundlicher Genehmigung des Rechenzentrums der Humboldt-Universität zu Berlin den RZ-Mitteilungen Nr. 15 (Dezember 1997) entnommen.
Autor: Alexander Geschonneck
geschonneck@rz.hu-berlin.de

SSH - dem Lauscher keine Chance

Im Normalfall wird heutzutage jede TCP/IP-Verbindung im Klartext übertragen. Dies betrifft nicht nur die Daten und die Bildschirmausschnitte, die transportiert werden, auch Login und Paßwort gehen so ungeschützt über das Netz. Jede Station, die sich zwischen dem eigenen Rechner und dem Zielrechner befindet, ist in der Lage, diese Informationen mitzuschneiden und zu mißbrauchen. Heutzutage sind in fast jeder UNIX-Distribution dafür geeignete Werkzeuge vorhanden. Viele davon sind sogar frei erhältlich. Daß dies jeden auch nur etwas sicherheitsbewußten Anwender schaudern läßt, dürfte wohl klar sein.

E-Mail und HTTP-Verbindungen kann man ohne Probleme verschlüsseln. Wie sieht es aber mit `telnet`, `rlogin`, `rsh`, `rdist` und `rcp` aus? Seit 1995 existiert ein finnisches Programm, das es sich zur Aufgabe gemacht hat, diese Problematik wirksam zu behandeln. Dieses Programm heißt **Secure Shell (SSH)**; sein Einsatz und die Installation sollen im folgenden Artikel näher beschrieben werden.

Mit SSH kann man sich über ein Netzwerk bei einem anderen Rechner anmelden, um dort Befehle auszuführen und Dateien zu transportieren. Es benutzt dabei eine starke Authentifizierung und ermöglicht eine sichere Kommunikation durch unsichere Kanäle.

Wovor SSH schützt

Durch den Einsatz von starker Authentifizierung werden folgende Gefahren eliminiert:

- *IP Spoofing*: Ein entfernter Host sendet Pakete, die vorgeben, von einem anderen eventuell vertrauenswürdigen Host zu kommen. SSH schützt auch vor gefälschten Paketen, die aus dem eigenen LAN stammen und vorgeben, daß sie vom eigenen Router kommen.
- *DNS spoofing*: Ein Angreifer fälscht Anworten eines DNS-Servers.
- *Sniffing*: Mitschneiden und Protokollieren von Verbindungsdaten und Paßwörtern (Abb. 1).
- *Hijacking*: Manipulation von Verbindungen durch Hosts, die als Vermittlungsstelle dienen oder im gleichen Segment liegen, z. B. durch Übernahme einer bestehenden Verbindung.
- *X attacks*: Attacken, die auf Abhören und Fälschen von X-Windows-Authentifizierungsdaten beruhen.

Mit anderen Worten, SSH traut niemals „dem Netz“. Jemand, der in ein Netzwerk eindringt, kann höchstens die SSH-Verbindung unterbrechen, aber nicht die Verbindung übernehmen, die übertragenen Daten mitlesen/mitschneiden und wieder einspielen. Dieser ganze Schutz beruht im wesentlichen auf Verschlüsselung. Daher sollte die vorhandene Option `-nocrypt` im Echtbetrieb niemals benutzt werden!

Wovor SSH nicht schützt

SSH wird niemals den normalen Schutz der Workstation oder des Servers übernehmen. Das heißt, wenn es jemandem gelingt, über bekannte Lücken oder durch Administrationsfehler Administratorrechte zu erlangen, kann er auch SSH kompromittieren. Wenn jemand unberechtigten Zugang zu HOME-Verzeichnissen hat, kann die Sicherheit, die SSH dem Nutzer bietet, wirkungslos sein. Dies betrifft vor allem HOME-Verzeichnisse, die per NFS zur Verfügung gestellt werden. NFS ist höchst unsicher und kann leicht kompromittiert werden. Im HOME-Verzeichnis eines jeden Nutzers werden im Unterverzeichnis `.ssh/` eigene Client-Konfigurationsdateien, die Public Keys der vertrauenswürdigen Server und der eigene Private Key gespeichert.

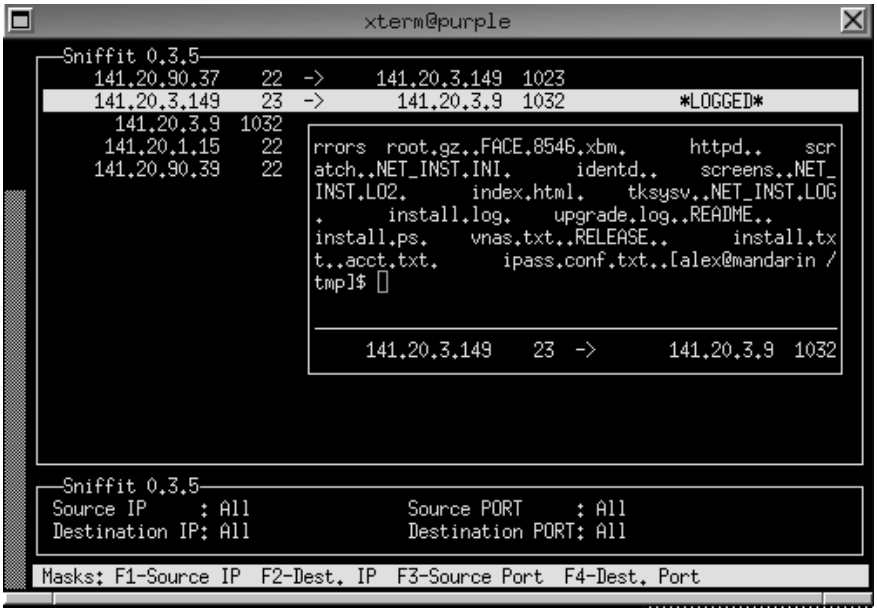


Abb. 1: Netzwerkmitschnitt ohne SSH

Es wird eine zusätzliche Authentifizierungsmethode eingeführt. Der bekannte und bekanntermaßen unzulängliche `.rhosts`-Mechanismus wird durch RSA Server-Authentifizierung ergänzt. Es ist auch eine pure RSA-Authentifizierung möglich.

Die gesamte Kommunikation zwischen Client und Server wird automatisch und – für den Anwender – transparent verschlüsselt. Diese Verschlüsselung schützt außerdem vor gefälschten Paketen und Versuchen, die Verbindung zu kapern. Unter X11 ist

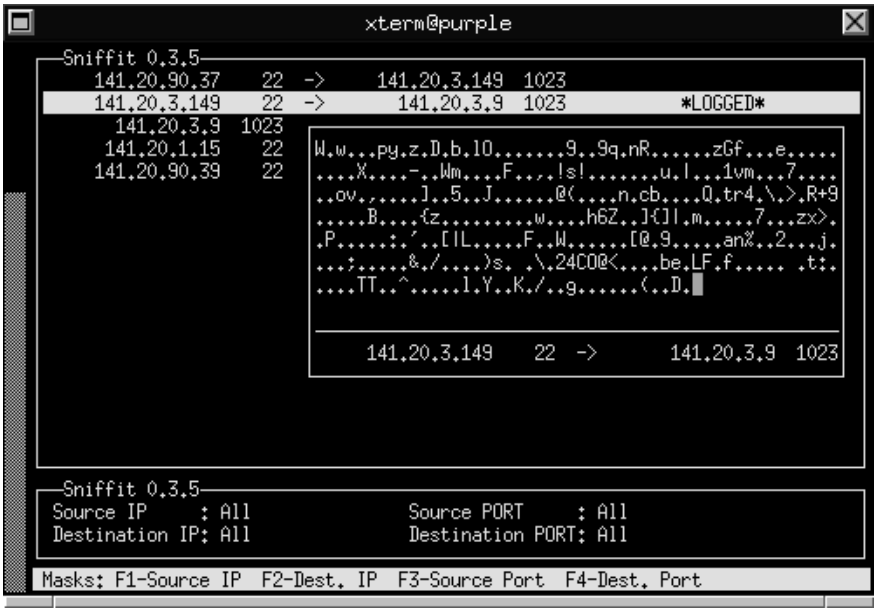


Abb. 2: Netzwerkmitschnitt mit SSH

darüberhinaus ein verschlüsseltes X-Forwarding möglich. Durch die RSA Host-Authentifizierung wird der Client bei jedem Verbindungsaufbau vor trojanischen Pferden, die durch gefälschte Routing- und DNS-Informationen eingeschleust werden können, geschützt. Durch die RSA Client-Authentifizierung wird der Server vor gefälschten Paketen geschützt, noch bevor er auf `.rhosts` oder `/etc/hosts.equiv` basierende Authentifizierung benutzt.

SSH ist als wirksamer, kompletter Ersatz für `rlogin, rsh, rcp` und `rdist` gedacht. In den meisten Fällen ist SSH auch ein `telnet`-Ersatz!

Funktionsweise

SSH benutzt ein paket-orientiertes, binäres Protokoll. Es wartet auf Port 22, der offiziell für SSH reserviert ist, auf Verbindungen. Das benutzte Protokoll tauscht zufällige Session Keys unter Einsatz des RSA-Algorithmus aus. Der Rest der Verbindung wird – je nach Konfiguration – mit `3DES, DES RC4-128, TSS` oder `Blowfish` verschlüsselt. RSA wird auch für die Authentifizierung benutzt. Der benutzte Session Key wird aber niemals auf der Festplatte gespeichert; er wird ständig neu erstellt und befindet sich ausschließlich im Hauptspeicher.

Wie läuft der Login-Prozeß ab?

Der SSH-Daemon kontrolliert den Login-Prozeß folgendermaßen:

1. Es wird die Lastlogin-Zeit und der Inhalt von `/etc/motd` (wenn nicht abgestellt) angezeigt.
2. Es wird die Loginzeit gespeichert.
3. Wenn die Datei `/etc/nologin` existiert, wird deren Inhalt angezeigt und die Verbindung beendet. Dies gilt nicht für root.
4. Es wird die UID des Nutzers angenommen.
5. Es werden die vorgegebenen globalen System-Umgebungsvariablen gesetzt.
6. Wenn `/etc/environment` und `~/.ssh/environment` existieren, werden auch die darin enthaltenen Umgebungsvariablen gesetzt.
7. Es wird in das Home-Verzeichnis des Nutzers gewechselt.
8. Wenn `~/.ssh/rc` oder `/etc/sshrc` existieren, werden sie ausgeführt.
9. wird `xauth` ausgeführt und `$DISPLAY` gesetzt (wenn nicht abgestellt).
10. Es wird die Nutzer-Shell gestartet.

Die wesentlichen Eigenschaften von SSH sind:

starke Authentifizierung

SSH kann reine RSA Host-Authentifizierung oder `.rhosts` zusammen mit RSA Host-Authentifizierung benutzen.

geschützte Privatsphäre

Automatische, für den Nutzer transparente Verschlüsselung der gesamten Verbindung. Host und Client Keys werden mit RSA verschlüsselt. Die Session wird je nach Konfiguration mit `3DES, DES` oder `IDEA` verschlüsselt. Die Verschlüsselung beginnt vor der Paßwortübertragung!

Abb. 3: Anmeldung mit slogin

sichere X11 Sessions

$DISPLAY wird auf dem Host gesetzt, und X11-Verbindungen werden automatisch über den verschlüsselten Kanal übertragen.

Port Forwarding

Bidirektionale Umlenkung von normalen TCP/IP-Ports auf die verschlüsselte Verbindung.

Automation

Die unsicheren alten r*-Programme werden komplett durch die neuen ersetzt. Der Nutzer kann wie gewohnt mit .rhosts arbeiten.

Vertraue niemals dem Netz

Ist RSA „eingeschaltet“, wird nur noch dem Privaten Schlüssel getraut.

Host Authentication Key

Der Client kann anhand des gespeicherten Server Keys den Server identifizieren.

User Authentication Key

Der Server kann anhand des gespeicherten Client Keys den Client identifizieren.

Server Key Regeneration

Der Session Key wird regelmäßig neu erstellt und niemals auf der Festplatte gespeichert.

Konfigurierbar

Client wie auch Server sind global und individuell nutzerbezogen konfigurierbar.

rsh Fallback

Wenn kein SSH-Daemon auf dem Zielsystem läuft, kann automatisch das alte (unsichere) r*-Protokoll benutzt werden.

Kompression

Daten können bei Bedarf vor der Übertragung automatisch komprimiert werden.

Installation und Konfiguration

SSH ist zum gegenwärtigen Zeitpunkt in der Version 1.2.20 vorhanden. Die Entwickler geben folgende Minimalplattformen für den Einsatz an:

386BSD 0.1; i386
AIX 3.2.5, 4.1, 4.2; RS6000, PowerPC
BSD 4.4; weitere Plattformen
BSD/OS 1.1, 2.0.1; i486
BSD/386 1.1; i386
BSDI 2.1; x86
ConvexOS 10.1; Convex
Digital Unix 4.0, 4.0A, 4.0B; Alpha
DGUX 5.4R2.10; DGUX
FreeBSD 1.x, 2.x; Pentium
HPUX 7.x, 9.x, 10.0; HPPA
IRIX 5.2, 5.3; SGI Indy
IRIX 6.0.1; Mips-R8000
Linux 1.2.x, 2.0.x Slackware 2.x, 3.x, RedHat 2.1, 3.0; i486, Sparc
Linux 3.0.3, 4.0; Alpha
Linux/Mach3, Macintosh(PowerPC)
Linux/m68k (1.2.x, 2.0.x, 2.1.x)
Mach3; Mips
Mach3/Lites; i386
Machten 2.2VM (m68k); Macintosh
NCR Unix 3.00; NCR S40
NetBSD 1.0A, 1.1, 1.2; Pentium, Sparc, Mac68k, Alpha
OpenBSD 2.0; x86.
NextSTEP 3.3; 68040
OSF/1 3.0, 3.2, 3.2; Alpha
Sequent Dynix/ptx 3.2.0 V2.1.0; i386
SCO Unix; i386 (Client)
SINIX 5.42; Mips R4000
Solaris 2.3, 2.4, 2.5; Sparc, i386
Sony NEWS-OS 3.3 (BSD 4.3); m68k
SunOS 4.1.1, 4.1.2, 4.1.3, 4.1.4; Sparc, Sun3
SysV 4.x; verschiedene Plattformen
Ultrix 4.1; Mips
Unicos 8.0.3; Cray C90
Windows (3.x/95/NT), MacOS, Amiga, OS/2

Das Programmpaket besteht aus folgenden Komponenten:

sshd

Server-Programm, „lauscht“ auf Port 22 auf Verbindungen von Clients, authentifiziert die Verbindungen und startet den Dienst

ssh

Client-Programm, dient zum Verbindungsaufbau mit sshd als rlogin- und rsh-Ersatz

slogin

symbolischer Link zu ssh (rlogin-Ersatz)

scp

kopiert Dateien zwischen SSH-Systemen (rcp-Ersatz)

ssh-keygen

erstellt Authentifizierungsschlüssel für Server und Nutzer

ssh-agent

Authentifizierungsagent; verwaltet online die RSA-Schlüssel

ssh-add

registriert neue Schlüssel beim ssh-agent

make-ssh-known-hosts

Perl-Script, das im Netzwerk nach öffentlichen Schlüsseln sucht und sie in /etc/ssh_known_hosts oder $HOME/.ssh/known_hosts speichert

Wenn ein Nutzer eine SSH-Verbindung zu einem SSH-System herstellen möchte, kann er u. a. folgende Kommandos auf der Befehlszeile eingeben:

```
% ssh Zielsystem Befehl_der_auf_dem_Zielsystem_
ausgeführt_werden_soll
```

oder

```
% ssh Zielsystem
```

oder

```
% xterm -e ssh Zielsystem &
```

Wenn das Zielsystem kein SSH installiert haben sollte, werden automatisch die adäquaten r*-Programme benutzt. Durch die Angabe der Option -C kann man eine Komprimierung der Verbindungsdaten erreichen. Das Starten der Programme mit der Option -v ermöglicht eine genaue Fehleranalyse durch erweiterte Bildschirmausgabe.

Die folgenden Konfigurationsdateien sind für den Einsatz von SSH von Bedeutung:

Verzeichnis	*Dateiname*	*Verwendung*
/etc/	ssh_host_key	privater Schlüssel des Servers; nur für root zugänglich
	ssh_host_key.pub	öffentlicher Schlüssel des Servers
	ssh_random_seed	Verweis für den systemweiten Zufallsnummerngenerator; nur für root zugänglich
	ssh_known_hosts	systemweite Liste mit bekannten öffentlichen Schlüsseln anderer Systeme; ein System pro Zeile
	ssh_config	systemweite Konfigurationsdatei für die SSH-Clients
	sshd_config	Konfigurationsdatei für den SSH-Server
	sshd.pid	Process-ID des letzten sshd-Prozesses
	nologin	wenn diese Datei existiert, darf sich nur root auf dem System anmelden; der Inhalt dieser Datei wird allen anderen Nutzern angezeigt, wenn sie abgewiesen werden
	environment	Umgebungsvariablen, die bei der SSH-Anmeldung gesetzt werden
	hosts.equiv	systemweite Definition von Nutzern und Hosts, die sich via rlogin/rsh anmelden dürfen, wenn RhostAuthentication oder RhostRSAAuthentication in der /etc/sshd_config gesetzt ist
	shosts.equiv	gleiche Funktion wie hosts.equiv, aber nur für SSH
	sshrc	beinhaltet Befehle, die bei der Anmeldung ausgeführt werden, bevor die Shell eines Nutzers gestartet wird
$HOME/	.rhosts	ermöglicht nutzerbezogene RhostAuthentication, wenn es in der /etc/config_sshd gesetzt ist
	.shosts	gleiche Funktion wie .rhosts, aber nur für SSH
	.Xauthority	wird von SSH benutzt, um das Authorization Cookie für den X11-Server zu speichern; SSH überprüft, daß die X11-Forward-Verbindungen dieses Cookie betreffen; wenn die X11-Verbindung aufgebaut wurde, wird dieses Cookie durch das richtige X11-Cookie ersetzt; alle X11-Verbindungen gehen automatisch durch diesen verschlüsselten Kanal, den der SSH-eigene X11-Proxy-Server bereitstellt; SSH setzt $DISPLAY auf den Server mit einer Displaynummer, die größer als 0 ist
$HOME/.ssh/	known_hosts	nutzerbezogene Liste mit bekannten öffentlichen Schlüsseln anderer Systeme; ein System pro Zeile; gilt als Ergänzung der systemweiten /etc/ssh_known_hosts, wenn StrictHostKeyChecking in /etc/sshd_config abgestellt ist.
	identity	privater Schlüssel des Nutzers; wird mit ssh-keygen erstellt und ist durch eine Passphrase geschützt
	identity.pub	öffentlicher Schlüssel des Nutzers; entsteht bei der Erstellung des privaten Schlüssels
	authorized_keys	nutzerbezogene Liste öffentlicher Schlüssel (identity.pub) von Nutzern, die ohne Angabe eines Paßwortes Zugang zu diesem Nutzer-Account haben
	random_seed	Verweis für den nutzerbezogenen Zufallsgenerator; sollte nur für den Nutzer lesbar / schreibbar sein und von ihm nicht verändert werden
	ssh_config	nutzerbezogene Konfigurationsdatei für den SSH-Client
	environment	Umgebungsvariablen, die bei der SSH-Anmeldung gesetzt werden; wird nach /etc/environment abgearbeitet
	rc	nutzerbezogene Variante von /etc/sshdrc

Angesichts der Gefahren, die herkömmliche telnet- oder rlogin-Verbindungen beinhalten, sollte sich jeder überlegen, diese überholten Programme durch verschlüsselungsfähige abzulösen. Installation, Konfiguration und Einsatz der Programme wie SSH sind einfach und gewährleisten Erfolg bei der sicheren Übertragung von Daten über unsichere Kanäle.

Diesen Artikel haben wir mit freundlicher Genehmigung des Rechenzentrums der Humboldt-Universität zu Berlin den RZ-Mitteilungen Nr. 15 (Dezember 1997) entnommen.
Autor: Alexander Geschonneck
geschonneck@rz.hu-berlin.de

Internet-Sicherheit von Windows-Rechnern

Das Internet ist in den letzen Jahren explosionsartig gewachsen. Die International Data Corporation (IDC) schätzt, daß im Jahr 2000 zweihundert Millionen Menschen das Internet nutzen werden – 1995 waren es ca. 35 Millionen. Jede Minute, jeden Tag verbinden sich weltweit immer neue Rechner oder ganze Netzwerke mit dem Internet. Laut einer Zählung, die von den „Network Wizards“ im Internet durchgeführt wurde, gab es im Juli '97 im DNS-Adressraum 19.540.000 Rechner. Ein Jahr zuvor waren es noch 12.881.000. Es scheint, daß sich jeder mit dem „Netz der Netze“ verbinden möchte. Die einfache Unterstützung der populärsten Internet-Protokolle durch Windows NT und Windows 95 tut ihr übriges: TCP/IP Protokoll laden, Router konfigurieren, einen Internet Provider aussuchen, und bevor der Nutzer es merkt, ist er Bestandteil des Internet – und somit potentielles Angriffsziel, wie die restlichen 19 Millionen Rechner.

Der so einfach ans Internet angeschlossene Rechner ist durch eben diese Verbindung nun neuen Gefahren ausgesetzt. Zu diesem Zeitpunkt hat der Nutzer sicherlich noch keine Vorstellung davon, wie es ist, am Sonntagmorgen um drei im Rechenzentrum nach „sauberen“ und aktuellen Backups suchen zu müssen, weil ein Hacker seine bzw. ihre Hand im internen Netzwerk hatte. Der folgende Artikel soll Ihnen zeigen, wie Sie diesen Alptraum verhindern können.

Eigentlich hat der sicherste Rechner keine Netzwerkkarte, keine Festplatte, ist ausgeschaltet und steht in einem verschlossenen, bewachten Raum. Leider ist dies nicht sehr sinnvoll. Ebensowenig sinnvoll ist allerdings ein ungesichertes System, das an das Internet angeschlossen ist und jedem anonymen Zugang zu seinen Ressourcen gestattet. Bevor Sie also Ihren Windows-Rechner an das Internet anschließen, sollten Sie wissen, wie Sie verhindern können, daß Ihre Daten gefährdet werden. Sie sollten genau planen, welchen Rechner Sie an das Internet anschließen und welche Daten sich darauf befinden sollen.

Sie sollten im Vorfeld
- herausfinden, was Sie zu schützen beabsichtigen,
- wissen, was Sie für diesen Schutz benötigen,
- bestimmen, welcher Aufwand für diesen Schutz notwendig ist,
- Maßnahmen einleiten, die Sie kostengünstig schützen, und
- Ihre Entscheidungen kontinuierlich überprüfen, um Ihre Schutzmaßnahmen den wechselnden Anforderungen anzupassen.

Bevor Sie sich nach Software umsehen, die Ihre Systemsicherheit erhöhen soll, nutzen Sie zuerst die Mittel und Methoden, die Ihnen Ihr Betriebssystem selbst liefert.

Windows NT bietet Schutzmöglichkeiten in vier grundlegenden Bereichen:

- log-on Authentisierung,
- Objektsicherheit,
- Nutzerrechte,
- Audit.

Wenn Sie diese Bereiche gut konfiguriert haben, sind Sie bestens für einen Anschluß an ein öffentliches Netzwerk gewappnet. Hier sind ein paar Tips, wie Sie Ihr NT/95-Netzwerk zu einem sicheren Bereich machen können.

Diese Liste ist wie immer unvollständig und soll als kleine Gedächtnisstütze dienen. Sie zeigt nur einen Teil der Dinge auf, über die Sie nachdenken sollten, wenn Sie Ihren Windows-PC oder Ihr Windows-Netzwerk an das Internet anschließen wollen.

1. Sie sollten `NTFS`- dem `FAT`-Dateisystem vorziehen. `NTFS` hat Sicherheitseigenschaften, die `FAT` nicht besitzt. Müssen Sie `FAT` aus irgendeinem Grund doch einsetzen, sollten keine Systemdateien auf diesem Dateisystem vorhanden sein. Sensitive Daten sollten ebenfalls nicht auf einem `FAT`-Dateisystem gespeichert werden. Sie können keine Zugriffs- und Eigentümerrechte an Dateien auf `FAT`-Dateisystemen definieren. Beim Exportieren solcher Dateisysteme ist der ganze Verzeichnisbaum gefährdet.

2. Stellen Sie sicher, daß alle betriebssystemeigenen Paßwortschutzoptionen aktiviert sind. Dies beinhaltet zwingend ein schwer zu erratendes Paßwort und sein Wechseln in regelmäßigen Zeitabständen. Auch ist es ratsam, den Namen des letzen angemeldeten Nutzers beim nächsten Logon zu verbergen. Windows NT kann Nutzerkonten automatisch sperren, nachdem mehrere falsche Paßwörter eingegeben wurden. Aktivieren Sie diese Option. Sie können damit verhindern, daß sich ein Eindringling durch sogenannte Brute Force Attacks Zugang zu Ihrem System veschafft. Fordern Sie Ihre Nutzer auf, schwer zu erratende Paßwörter zu wählen. Solange Microsoft nicht die Verschlüsselung der `SAM`-Datenbank (Security Account Manager) ändert, ist es ratsam, Paßwörter von zwischen sechs bis acht Zeichen Länge zu wählen. Dies erhöht die Zeit, die ein Eindringling braucht, um ein Paßwort zu erraten. Brute Force Attacks auf Paßwörter sind heute eine sehr populäre Methode, um in Netzwerke einzudringen. Es ist ebenfalls ratsam, die Datei `PASSFILT.DLL` zu installieren, die mit dem Windows NT Servicepack 2 und 3 ausgeliefert wird. Sie können mehr über diese DLL in den Microsofts Knowledge Base-Artikeln und den `README`-Dateien der Servicepacks erfahren.

3. Es ist kein Geheimnis, daß der Administrator-Account Ziel für die meisten Angriffe ist. Erstellen Sie einen neuen Administrator-Account und übertragen Sie alle Rechte vom existenten Administrator-Account auf den neuen. Geben Sie diesem neuen Account einen unscheinbaren Namen. Entziehen Sie dem alten Administrator-Account alle Rechte, löschen Sie ihn jedoch nicht. Ein Eindringling wird sehr viel Zeit aufwenden, in diesen Account einzubrechen.

4. Verringern Sie die Zahl der Nutzer, die zur Administratorgruppe gehören. Erteilen Sie niemandem aus Bequemlichkeit Administratorrechte und überprüfen Sie die Mitglieder der Administratorgruppe regelmäßig.

5. Aktivieren Sie das Auditsystem auf allen Windows NT Rechnern. Im Bereich Audit im User Manager können Sie eine Audit Policy für jeden Nutzer oder jede Nutzergruppe definieren. Mit Hilfe des Explorers können Sie ein objektbezogenes Audit konfigurieren.

6. Seien Sie sehr vorsichtig beim Aktivieren von `NT Domain Trusts`. Diese Konfigurationen können in größeren NT-Netzwerken schnell außer Kontrolle geraten, zumal, wenn dieses Vertrauen wechselseitig besteht.

7. Deaktiveren Sie `NetBIOS über TCP/IP`, wo immer Sie können. Dies betrifft besonders Ihre Windows-Rechner, die als Gateway zum Internet dienen.

8. Deaktivieren Sie alle nicht benötigten TCP/IP Ports (`Inbound` und `Outbound`). Achten Sie besonders darauf, daß die UDP Ports `137` und `138` und der TCP Port `139` auf Ihren Gateways, Routern und Firewall-Systemen blockiert werden. Dies verhindert bekannte und auch neue Attacken aus dem Internet auf Ihr Windows-Netzwerk.

9. Deaktivieren Sie die Option `Access from Network` (mittels des `User Managers`) für alle Nutzer, die diesen Zugang nicht unbedingt benötigen. Diese Nutzer können dann nur noch lokal an der Konsole arbeiten.

10. Überprüfen Sie in regelmäßigen Zeitabständen Ihr System auf überflüssige Nutzer-Accounts. Setzen Sie für alle temporären Accounts ein Verfallsdatum und erteilen Sie Rechte vorsichtig.

11. Informieren Sie Ihre Nutzer durch Hinweise beim Logon, daß der Zugang zu Ihren Systemen nur authorisierten Nutzern gestattet ist, daß Protokollierungen stattfinden und jeder Verstoß gegen Ihre Sicherheitsrichtlinien überprüft und gegebenenfalls juristisch verfolgt wird. In vielen Fällen ist es selbst in Ihrem privaten Netzwerk datenschutzrechtlich bedenklich, Netzverbindungsdaten zu protokollieren und auszuwerten. Dieser Hinweis könnte Sie vor juristischen Problemen schützen. Die Warnung sollte nicht nur auf Ihrem Logon-Bildschirm, sondern auch auf Ihren WWW- und FTP-Servern erscheinen.

12. Stellen Sie sicher, daß Ihre Nutzer ihre Windows-Workstations nicht im eingeschalteten Zustand unbeaufsichtigt lassen. Überall sollten paßwortgeschützte Bildschirmschoner aktiviert sein. Erziehen Sie Ihre Nutzer dazu, sich abzumelden, wenn Sie für längere Zeit die Workstation verlassen. Es ist auch ratsam, die Windows-Workstations über Nacht und an Wochenenden auszuschalten. Dies könnte helfen, die Zahl der illegalen Modem-, FTP- und WWW-Server einzudämmen.

13. Ein Gast-Account wird bei jeder Windows NT-Installation automatisch eingerichtet. Wenn möglich, sollten Sie diesen Account entfernen. Bei Bedarf sollten Sie sich die Zeit nehmen, einen temporären Gast-Account zu erstellen. Wenn Sie den Microsoft Internet Information Server (IIS) installieren, wird automatisch ein spezieller Gast-Account `IUSR_Rechnername` eingerichtet. Dieser Nutzer kann sich lokal anmelden. Wenn Sie keinen anonymen Zugriff auf Ihren WWW-Server haben wollen, sollten Sie diesen Account entfernen.

14. Überwachen Sie Ihr Netzwerk engmaschig. Es gibt immer wieder Fälle, bei denen ein Einbruch nicht bemerkt wird, weil kein Netzmonitor oder Intruder Detection System im Netzwerk installiert war.

15. Stellen Sie sicher, daß die Router und Gateways zwischen Ihrem privaten und dem öffentlichen Netzwerk `Source Routing`, `IP Spoofing` und `ICMP Redirects` verhindern können und es auch tun. Es kann auch nicht schaden, Software einzusetzen, die einen Netzwerkscan aus dem Internet verhindert.

16. Deaktivieren Sie die einfachen TCP/IP-Dienste auf Ihrem Windows Rechner. Dies stoppt Dienste wie `chargen`, `echo`, `daytime`, `discard` und `qotd`. Diese Dienste eignen sich exellent, um Ihren Rechner mit einer Denial-of-Service Attack lahmzulegen.

17. Auf Ihrem Windows-Rechner sollten keine Dienste laufen, die Sie nicht unbedingt brauchen. Solche Dienste sind immer wieder gezielten Attacken ausgesetzt.

18. Versuchen Sie, Ihre Nutzer zum Mitdenken zu erziehen. Führen Sie regelmäßig Schulungen und Weiterbildungen durch.

Ausgehend vom derzeitigen Entwicklungstand, sollten Sie diese Hinweise beachten, bevor Sie einen Windows 95- oder Windows NT-Rechner ungeschützt mit einem öffentlichen Netz wie dem Internet verbinden.

Diesen Artikel haben wir mit freundlicher Genehmigung des Rechenzentrums der Humboldt-Universität zuBerlin den RZ-Mitteilungen Nr. 15 (Dezember 1997) entnommen.
Autor: Alexander Geschonneck
geschonneck@rz.hu-berlin.de

Sicherheitsrisiken mit aktiven Webseiten

Mit dem World Wide Web, das 1989 im CERN entworfen wurde, entstand ein Netz miteinander verbundener Hypertext-Dokumente. Der Benutzer kann sich über die Verweise in den Dokumenten im Hypertext-Raum bewegen. Der Nachteil dieser Arbeitsweise bestand darin, daß der Benutzer wenig Möglichkeiten der Interaktion hatte. Deshalb waren spätere Erweiterungen darauf gerichtet, dieses Medium interaktiv benutzbar zu machen. Dazu ist es notwendig, daß der Benutzer Eingaben in das System vornehmen kann, die mit Hilfe von Programmen verarbeitet werden und entsprechende Reaktionen und Antworten erzeugen. Die erste Möglichkeit wurde mit der Einführung der Formularbefehle und des „Common Gateway Interface“ (CGI) geschaffen. Hierbei werden die Daten, die der Benutzer in das Formular einträgt, über das Netz zum Server transportiert. Auf diesem wird dann ein Programm gestartet, das die Verarbeitung übernimmt. Es soll hier nicht weiter auf dieses Prinzip eingegangen werden, da die Sicherheitsprobleme vor allem im Server auftreten und vom Administrator gelöst werden müssen. Der Benutzer solcher Formulare sollte nur bedenken, daß die eingegebenen Daten im allgemeinen ungeschützt über das Netz transportiert werden. Es besteht dadurch die Möglichkeit, daß sie während des Transportes gelesen und auch geändert werden können.

Ein weiterer Schritt in der Entwicklung des WWW bestand darin, daß die Möglichkeit geschaffen wurde, Programme in die Dokumente einzubinden. Sie werden beim Aufruf der entsprechenden Seiten vom WWW-Server zum lokalen Rechner transportiert und häufig, ohne den Nutzer davon zu informieren, dort gestartet. Dies birgt natürlich die Gefahr, daß Programme geladen werden, die wissentlich oder unwissentlich Funktionen enthalten, die den lokalen Rechner schädigen oder vertrauliche Informationen dieses Rechners weitergeben. Deshalb müssen Sicherheitsmechanismen eingeführt werden, die dies verhindern. Für die Erstellung der Programme werden die Sprachen Java und JavaScript eingesetzt. Nachfolgend sollen die Besonderheiten dieser Sprachen hinsichtlich der Sicherheit gezeigt werden.

Java

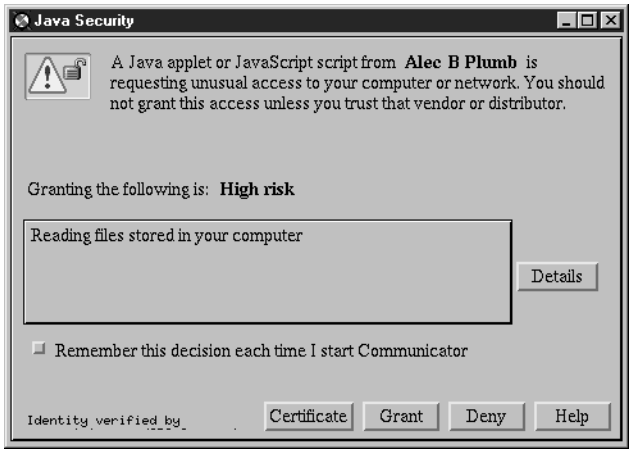
Java wurde als allgemeine, objektorientierte Programmiersprache von der Firma Sun Microsystems entwickelt. Ein großer Vorteil der Sprache besteht darin, daß die Programme, die mit Hilfe dieser Sprache geschrieben wurden, auf (fast) allen Rechnertypen direkt abgearbeitet werden können. Das wird dadurch erreicht, daß der Quellcode in einen rechnerunabhängigen Code (Bytecode) übersetzt wird. Dieser wird dann von einem virtuellen Rechner (Java Virtual Machine) interpretiert und dadurch abgearbeitet. Bei der Definition der Programmiersprache wurde darauf geachtet, daß sie möglichst wenig Elemente enthält, die zu fehlerhaften Programmen führen können. Andererseits soll es aber möglich sein, Java-Programme zu erstellen, die beliebige Funktionen im Computer ausführen können. Dazu ist es notwendig, daß auch auf die lokalen Ressourcen (lokale Festplatte, Netzwerk u. a.) zugegriffen werden kann. Es wäre aber ein sehr hohes Risiko, solche Programme aus dem anonymen Internet zu laden. Deshalb wurden den Programmen, die in den WWW-Dokumenten eingebettet sind (sog. Applets), bisher folgende Beschränkungen auferlegt:

- Applets dürfen keine Dateien auf dem lokalen Rechner lesen oder schreiben.
- Applets können keine Netzwerkverbindungen zu anderen Rechnern als dem, von dem sie geladen wurden, aufbauen.
- Applets können keine Programme starten.
- Applets können keine Programmbibliotheken laden.
- Applets haben nur begrenzten Zugriff zu den Systeminformationen des lokalen Rechners.

Diese auch als „Sandbox“ bezeichnete Methode soll dazu führen, daß die von einem unbekannten Server des Internets geladenen Programme keinen Schaden auf dem lokalen Rechner anrichten können. Die Überwachung der oben genannten Einschränkungen übernimmt der Browser, in dem ein Java-Interpreter (Bytekode-Interpreter) integriert ist. Damit wird auch deutlich, daß die Sicherheit bei dieser Methode davon abhängt, wie sorgfältig diese Überwachungsfunktionen im Browser implementiert wurden. Die Vergangenheit hat gezeigt, daß immer wieder Sicherheitslücken in einzelnen Browserversionen aufgetreten sind, die dazu führen konnten, daß spezielle Applets Zugriff auf die lokale Festplatte erhielten oder andere unerwünschte Funktionen ausführten [1] [2].

Die Sandbox-Methode hat aber auch den Nachteil, daß eventuell nützliche Funktionen mit Applets nicht realisiert werden können, wenn dazu Zugriffe auf die lokalen Ressourcen des Rechners benötigt werden. Deshalb hat die Firma Netscape für ihren Browser der Version 4 (Communicator 4.0x) die Sicherheitsstrategie geändert. Die Applets können eine digitale Unterschrift vom Hersteller erhalten. Diese Unterschrift wird aus einer Art Prüfsumme vom Programm und einem persönlichen Schlüssel des Unterzeichners gebildet. Dadurch kann ein unterschriebenes Programm nachträglich nicht unbemerkt geändert werden. So unterschriebene Applets können dann einen erweiterten Zugriff auf lokale Ressourcen anfordern. Der Browser erkennt bei der Sicherheitsprüfung diese Funktionen und meldet sie dem Benutzer, wobei

gleichzeitig eine Information zur Unterschrift und zum Unterzeichner angezeigt wird (siehe Bild).



Der Benutzer kann dann entsprechend seinem Vertrauen zum Programmierer entscheiden, ob diese Funktion ausgeführt werden soll. Der Vorteil dieser Methode besteht darin, daß es unwichtig ist, auf welchem Server sich das Objekt befindet und auf welchem (unsicheren) Wege es zum Benutzer gelangt, da es durch diese Unterschrift vor Veränderung geschützt ist. Die Schwierigkeit für den Leser besteht darin, einzuschätzen, welchem Programmierer von Applets er vertrauen kann.

JavaScript

JavaScript ist eine objektbasierte Sprache, die zur Einbindung von Programmen in HTML-Dokumenten dient. Sie wurde von der Firma Netscape zunächst unter dem Namen Live-Script entwickelt. Ziel war es, eine Programmiersprache zu schaffen, die es auch nichtprofessionellen Programmierern erlaubt, schnell einfache Programme zu schreiben. Um eine gewisse Ähnlichkeit mit der Sprache Java zu suggerieren, wurde sie später in Java Script umbenannt. Trotz mancher vergleichbarer Eigenschaften gibt es auch entscheidende Unterschiede. Der wohl auffälligste besteht darin, daß JavaScript als Quelltext (Script) in die HTML-Dokumente eingebunden wird. Diese Scripte werden nach dem Einlesen des Dokuments vom Browser interpretiert und abgearbeitet. Die Sicherheitsstrategie besteht darin, daß die Sprache keine Elemente enthält, die einen Zugriff auf die lokale Festplatte ermöglichen. Trotzdem sind auch hier Sicherheitslücken aufgetreten. Diese sind aber mehr dem Bereich der Verletzung der Privatsphäre zuzuordnen, d. h. es können Informationen über den lokalen Rechner oder über den Nutzer unbemerkt abgerufen werden. So haben Mitarbeiter der Bell Labs im Juli diesen Jahres einen Fehler in den Browsern von Microsoft wie auch Netscape entdeckt, der dazu führt, daß von einem Dokument ein JavaScript-Programm gestartet werden kann, das, selbst nachdem diese Seite verlassen wurde, die Internet-Aktivitäten des Benutzers sammelt und versendet [3]. Dabei kann protokolliert werden, welche Seiten (URL) später besucht wurden. Weitaus gefährlicher ist aber, daß auch das Ausfüllen von HTML-Formularen überwacht werden kann. Da dies direkt auf dem lokalen Rechner des Nutzers geschieht, kann dieser Eingriff auch nicht durch einen Firewall-Rechner oder durch Verschlüsselung der Formulardaten während der Datenübertragung verhindert werden. In den neuesten Versionen der Browser wurde dieser Fehler beseitigt. (Keine Lösung gibt es für Netscape Navigator Version 2.0x.)

Zusammenfassend kann festgestellt werden, daß trotz aller Begrenzungen für die Internet-Programme zur Zeit nicht mit Sicherheit verhindert werden kann, daß Java- oder JavaScript-Programme, die gemeinsam mit den Dokumenten geladen und automatisch gestartet werden, dem Nutzer schaden können. Deshalb sollten folgende Hinweise beachtet werden:

- Bei Computern, die sicherheitsrelevante Daten enthalten, sollten die Funktionen Java und JavaScript im Browser ausgeschaltet werden.
- Wer Java und JavaScript nutzen will, sollte immer die neueste Version eines Browser installieren, da dann zumindest die bekannten Sicherheitslücken beseitigt sind.
- Jede Warnung oder Meldung des Browsers sollte aufmerksam gelesen werden, bevor sie akzeptiert wird.

Die Informationen zur Sicherheit beim Browsen in HTML-Dokumenten gelten auch für das Lesen von Mails mit Hilfe des Netscape Navigators. Es können vollständige HTML-Dokumente inklusive entsprechender Java- oder JavaScript-Programme in eine Mail integriert werden. Wenn sie vom Mail-Programm des Browsers geöffnet werden, werden diese Programme gestartet.

Cookies

Eine weitere Funktion im WWW, die häufig Anlaß für Diskussionen zur Sicherheit bietet, sind die sog. „Cookies“. Das sind kleine Informationseinheiten, die vom WWW-Server an den Browser gesendet werden. Darin sind enthalten der Domain-Name des Servers, der Pfad auf dem Server, ein Verfallsdatum, der Name des Eintrags und ein variabler Teil. Diese Information wird zunächst im Browser gespeichert. Erst wenn der Browser geschlossen wird und das Verfallsdatum noch nicht erreicht wurde, wird ein Cookie auf die Festplatte des lokalen Rechners gespeichert (Datei `cookies.txt` unter MS Windows oder `cookies` unter UNIX). Bei jedem Verbindungsaufbau mit einem Server, dessen Cookies gespeichert sind, werden diese zum Server übertragen. Damit soll ein Nachteil des Übertragungsprotokolls (HTTP) überwunden werden, der darin besteht, daß es keine permanente Verbindung zwischen WWW-Server und lokalem Rechner gibt. Jeder neue Aufruf einer Seite oder das

Absenden eines ausgefüllten Formulars ist eine eigenständige Übertragung, wobei keinerlei Informationen zu vorherigen Verbindungen mitgeliefert werden. Hierdurch ist es schwierig, komplexe, mehrstufige Formulare aufzubauen. Der Einsatz von Cookies ermöglicht es, den Zustand einer Verbindung zu speichern und bei der nächsten Datenübertragung an den Server zu senden, so daß seine Reaktion sowohl von der aktuellen als auch von vorherigen Anfragen abhängen kann.

Die Gefahren durch Cookies bestehen darin, daß auf dem Server eine Statistik über den Besuch der einzelnen Seiten und somit über die Vorlieben des Benutzers geführt werden kann. Weiterhin werden dadurch Übertragungs- und Speicherkapazität gebunden. Durch die Definition einer maximalen Anzahl und Größe von Cookies wird dieses Problem aber begrenzt [4]. Abgesehen von der oben erwähnten Statistik stellen Cookies kein Sicherheitsrisiko dar. Trotzdem bieten die modernen Browser von Microsoft und Netscape die Möglichkeit, das Schreiben von Cookies zu verbieten.

Literatur:

[1] ZDNet News: Vorsicht: Platten-Crash beim Explorer. `http://www.pcpro.de/news/artikel/1997/09/09002-wf.htm`

[2] Sun Microsystems, Inc.: Chronology of security-related bugs. `http://www.javasoft.com/sfaq/chronology.html`

[3] Vinod Anupam: JavaScript Related Browser Vulnerability. `http://www-db.research.bell-labs.com/user/anupam/vulnerability/`

[4] Netscape Communications Corporation: Persistent Client State HTTP Cookies. `http://home.netscape.com/newsref/std/cookie_spec.html`

Diesen Artikel haben wir mit freundlicher Genehmigung des Rechenzentrums der Humboldt-Universität zu Berlin den RZ-Mitteilungen Nr. 15 (Dezember 1997) entnommen.

Autor: Lothar Wendroth
wendroth@rz.hu-berlin.de

Einstellung von Services im Bereich Kommunikation

Vom EDV-Zentrum wurde die Einstellung folgender – bisher vom Bereich Kommunikation betriebener – Services beschlossen.

Proxy/Caching-Service

Mit 30. Juni 1998 wird als Ergebnis einer Kosten/Nutzen-Überlegung das Proxy/Caching-Service auf `proxy.tuwien.ac.at` Port 8000 eingestellt. Bitte konfigurieren Sie so bald wie möglich Ihren Browser entsprechend („*Direct connection to the Internet*“).

Trotz einer guten Hitrate (45% der Zugriffe, 30% der Datenmenge) konnte nur eine Ersparnis an Internet-Bandbreite in der Größenordnung von 50.000 öS pro Jahr erzielt werden, deutlich weniger als die Kosten für dieses Service. Ursache für dieses schlechte Kosten/Nutzen-Verhältnis ist die zu geringe Verwendung des angebotenen Services, nur etwa 15% aller an der TU Wien ankommenden WWW-Daten gehen zur Zeit über den Proxy-Server.

Für Studenten und Angehörige der TU Wien, die den TeleWeb-Zugang der Fa. Telekabel verwenden, ist ein rudimentärer Proxy-Server (Socks5-Software, kein Caching) vorgesehen (siehe auch Seite 6).

Mail-Telefax-Gateway

Mit 30. Juni 1998 wird das Mail-Telefax-Gateway am Rechner `telefax.tuwien.ac.at` eingestellt. Als Alternative stehen diverse kommerzielle Fax-Gateways zu Verfügung (z.B. DATAKOM AUSTRIA, URL `http://www.datakom.at`).

Gopher-Service

Ende März 1998 wurde das Gopher-Service am Informationsserver der TU Wien (`info.tuwien.ac.at`, `gopher.tuwien.ac.at`) eingestellt. Bitte verwenden Sie das WWW-Service unter der URL `http://info.tuwien.ac.at`. Die Daten der Universitätsdirektion und der Bibliothek sind – zusätzlich zum WWW-Service – auch weithin über anonymous ftp abrufbar: `ftp://info.tuwien.ac.at/ud` bzw. `ftp://info.tuwien.ac.at/ub`

Ende April 1998 wurde auch das Gopher-Service am Informationsserver des Bereichs Kommunikation (`gopher://nic.tuwien.ac.at:70`) eingestellt. Bitte verwenden Sie unser WWW-Service unter der URL `http://nic.tuwien.ac.at`. Die Abfrage der TU-NET-Datenbank über das Gopher-Gateway ist weiterhin möglich:
`gopher://nic.tuwien.ac.at:4320/1device`

DECnet-Service

Ende März 1998 wurde – wegen des nicht existierenden Bedarfs – der DECnet Nameserver am Rechner ENAMED eingestellt. Die DECnet Knotentabelle der TU Wien steht weiterhin an der gewohnten Stelle `ftp://nic.tuwien.ac.at/netinfo/decnet/tu-nodes` zur Verfügung. Weiters kann unter VMS die aktuelle Knotentabelle mit dem Befehl

```
NCP COPY KNOWN NODES FROM EVAXSW TO BOTH
```

geholt werden.

Wegen der geringen Bedeutung des DECnet Gateway für Mails wird dieses Service am Mail Router der TU Wien (`mr.tuwien.ac.at`) mit der demnächst fälligen Umstellung auf Solaris eingestellt. Bitte geben Sie daher ab sofort Ihren Mail-Partnern nur mehr Mailadressen mit dem TCP/IP Namen Ihres Rechners (also ohne dnet) und informieren Sie Ihre Mail-Partner von der bevorstehenden Änderung der Adresse. Bitte ändern Sie auch eventuell in den White Pages eingetragene Adressen auf die entsprechenden TCP/IP Namen.

Datex-P Service

Ende März 1998 wurde das Datex-P Service (Zugang zur TU Wien, Zugang von der TU Wien zu anderen Datex-P Systemen) eingestellt. In den letzten Jahren wurde dieses Service nur von ganz wenigen Benutzern genutzt und verursacht in Relation zur Verwendung sehr hohe Kosten. Falls Benutzer in einzelnen Fällen den Zugang zu Rechnern außerhalb der TU Wien über Datex-P benötigen, so bietet DATAKOM AUSTRIA (URL `http://www.datakom.at`) ein ähnliches kommerzielles Service an.

Manfred Schenner

ÖBB Fahrplan online im Internet

Dem Beispiel ausländischer Bahnen folgend ist der Fahrplan der ÖBB nun auf einer eigenen Homepage im Internet über

`http://www.oebb.at/`

online am Computer abrufbar. Auch andere Informationen der ÖBB sind dort zu finden. Probieren Sie es einfach einmal aus.

Johann Kainrath

Neue Chemie-Datenbanken und Datenbank-Versionen

Die ISIS-Datenbanken

In einem gemeinsamen Projekt zwischen dem Institut für Organische Chemie und der Bibliothek der TU Wien wurden die ISIS-Software und eine Reihe der verfügbaren ISIS-Datenbanken der Firma MDL Information Systems für die TU Wien angeschafft. Das EDV-Zentrum hat sich bereit erklärt, eine entsprechende Systemplattform dafür zur Verfügung zu stellen, die Datenbanken wurden am Serversystem `fbch.tuwien.ac.at` (SGI Power Challenge L) implementiert.

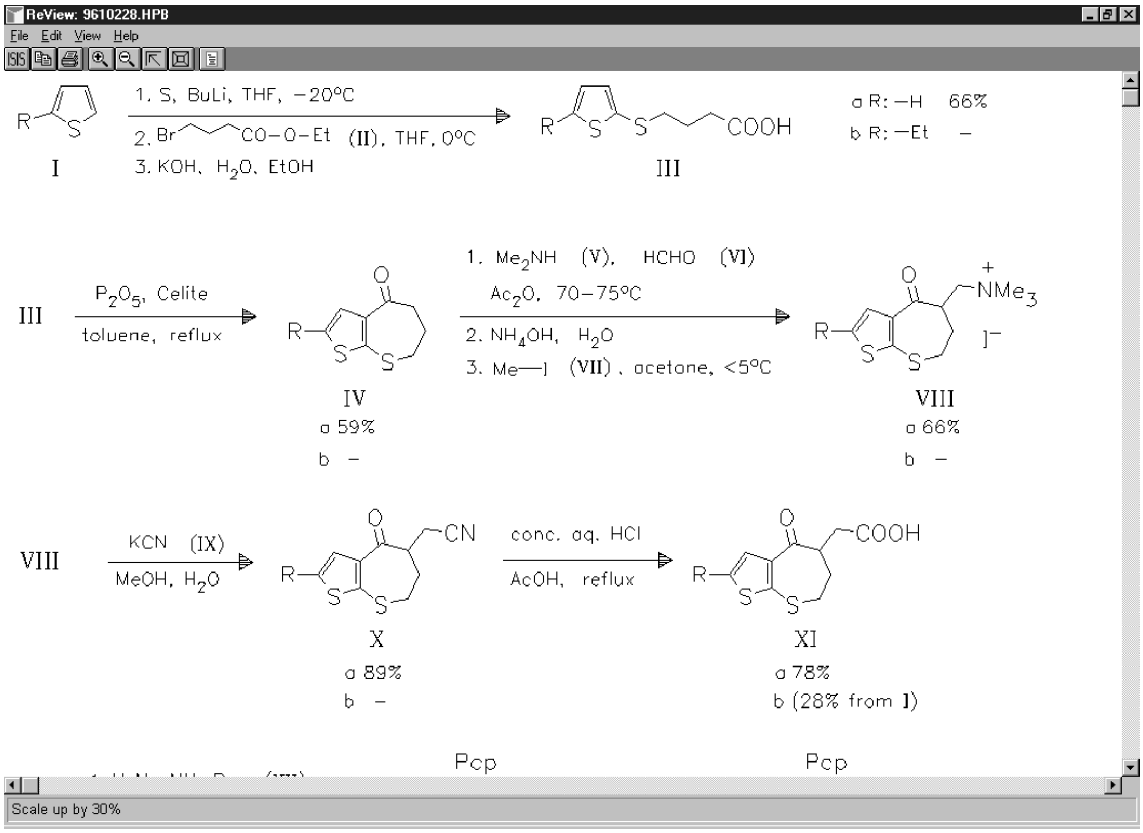
Die Verträge wurden so gestaltet, daß neben dem Zugriffsrecht für Institute der TU Wien auch andere österreichische Universitäten sich beteiligen können. Diese Möglichkeit wurde auch schon von Chemie-Instituten der Universität Wien sowie der Universitäten in Graz, Linz und Innsbruck genützt.

Das ISIS-Paket besteht einerseits aus der Server-Software ISIS-Host Version 2.1.2, welche auf dem Server `fbch` implementiert ist und in nächster Zeit auf ISIS-Host Version 3.0 gebracht wird, und aus einer Reihe von Client-Programmen für PCs und Workstations, andererseits aus den ISIS-Datenbanken.

An Client-Software stehen ISIS/Base mit ISIS/Draw, welche als universelle Clients für viele der vorhandenen Datenbanken verwendet werden können sowie der Reaction Browser und der Metabolite Browser für jeweils einen bestimmten Datenbank-Typ zur Verfügung. Die Clients sind für Windows-Systeme, teilweise auch für MacIntosh und für SGI IRIX Workstations verfügbar.

Derzeit werden folgende Datenbanken angeboten:

- Available Chemicals Directory (ACD3D) – beinhaltet alle käuflich verfügbaren Chemikalien.
- Comprehensive Heterocyclic Chemistry (CHC) – beinhaltet alle seit 1983 veröffentlichten Reaktionen der Heterozyklischen Chemie.
- ChemInform Reaction Library (CIRXL) – ersetzt den bisherigen wöchentlich erschienenen Chemischen Informationsdienst ChemInform und setzt sich aus den Jahrgängen 1992 bis 1998 zusammen mit bis zu 3 Updates pro Jahr. Insgesamt werden 64038 Reaktionen und 85046 Moleküle beschrieben.
- MDL Drug Data Report (MDDR3D) – enthält dreidimensional suchbare Strukturen.
- Metabolite (METAB) – enthält Informationen über Metabolismus von organischen Verbindungen und Pharmazeutika.



Graphische Darstellung einer Reaktion aus der Reaction Library

- National Cancer Institute Database (NCI3D) – enthält Daten vor allem für Pharmazeuten und Mediziner.
- ORGSYN – enthält Daten über Experimente der organischen Synthese.
- Reference Library of Synthetic Methodology (REFLIB) enthält innovative Reaktionen aus der Synthese-Literatur von 1946 bis 1990.

Für fachliche Auskünfte und Fragen bezüglich der Benützung der Client-Software stehen die Herren H. Krebs und Prof. U. Jordis am Institut für Organische Chemie zur Verfügung; für Fragen der Host-Software und der am `fbch` installierten Datenbanken bekommen Sie Auskunft bei H. Mastal am EDV-Zentrum. Ich möchte auch noch auf die WWW-Seite `http://perdix.tuwien.ac.at/isis/` hinweisen, die vom Institut für Organische Chemie betreut wird. Accounts für den Zugriff auf ISIS-Datenbanken werden vom EDV-Zentrum eingerichtet, wenn die Zustimmung von Prof. Jordis gegeben ist.

MassLib

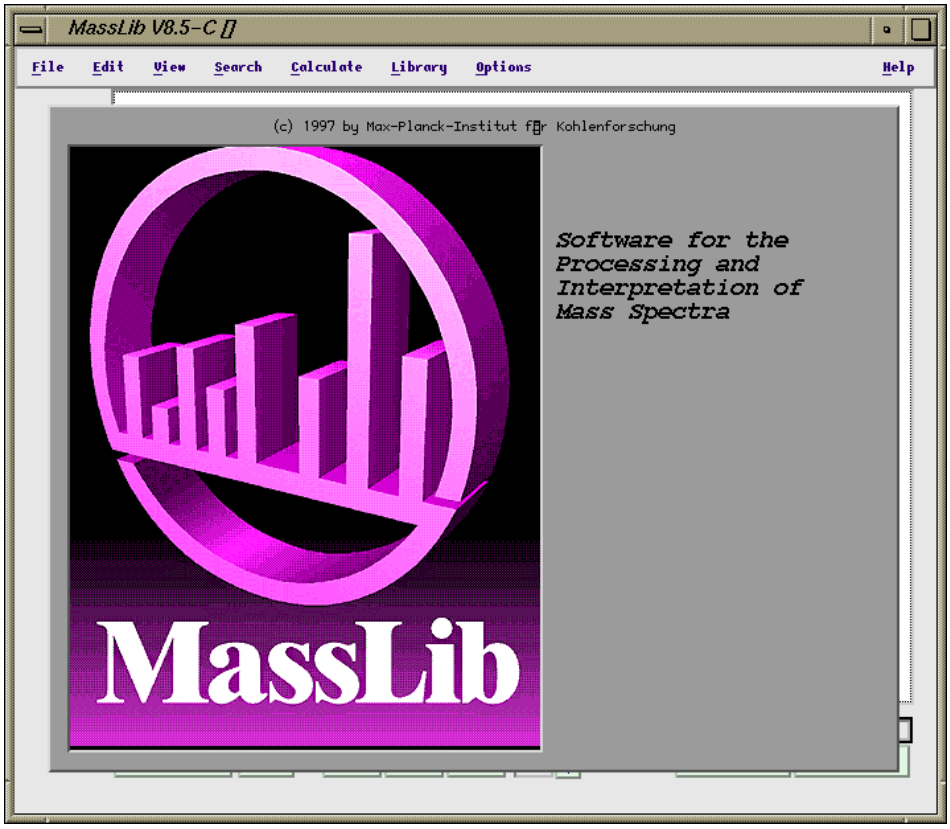
MassLib V8.5-C ist eine datenbank-orientierte Software zur Untersuchung von Massenspektren. MassLib wurde von verschiedenen Herstellern entwickelt; die derzeitige Weiterentwicklung und Anpassung für SGI stammt vom Max-Planck-Institut für Kohlenforschung in Mühlheim/Ruhr. Die Verwendung erfolgt über eine X-Oberfläche, die mit MassLib aufgerufen wird. MassLib kann in der momentanen Implementierung an der TU Wien die Libraries MPI-Lib mit 17 400 Eintragungen und Wiley mit 130 000 Eintragungen durchsuchen.

Da die Software-Lizenz an das Institut für Allgemeine Chemie, Abt. für Chemometrie gebunden ist, benötigen Interessenten die Zustimmung von Prof. Varmuza (E1523) für die Benützung von MassLib.

Cambridge Structural Database

Seit 30. April steht die Cambridge Structural Database Version 5.15 (released April 1998) am Server `fbch` zur Verfügung. Die mitgelieferte Brookhaven Protein Databank ist am Stand Februar 1998. Neben einzelnen kleineren Korrekturen gibt es neue Features bei Prequest und Pluto. Die Koordinaten-Files der PDB haben bereits einen Umfang angenommen, der eine CD übersteigen würde. Es wurden daher in der Version 5.15 einzelne Koordinaten-Files weggelassen (NMR und theoretische Modelle). Wir haben die fehlenden Koordinaten-Files, soweit möglich, aus der Version 5.14 ergänzt.

Helmut Mastal



Prozessortausch und Betriebssystemupgrade am Vektorrechner NEC SX-4

In der ersten Märzwoche wurden die Prozessoren mit einer bisherigen Taktrate von 8,8 ns (das entsprach einer Peak-Performance von 1,8 GFlops) auf einen schnelleren Typ mit einer Taktrate von 8 ns (2 GFlops pro Prozessor) ausgetauscht. Dieser Austausch erfolgte zugleich mit der gesamten Zentraleinheit, sodaß die Bezeichnung der Rechnertype nun SX-4A ist.

Neben den Hardware-Umbauarbeiten wurden Änderungen an der Netzwerkanbindung und ein Systemupgrade auf SUPER-UX R7.1 Rev1 durchgeführt. Auch die Compiler wurden auf den Stand 7.1 angehoben !

In weiterer Folge wurden die letzten Modifikationen an Systemprodukten (wie ksh, csh, make, cut, find etc.), den Compilern (C, FORTRAN 77/90) und NQS installiert.

Erwin Srubar

Hardwaretausch am Server `mail.zserv`

Anfang April wurde das bestehende RISC System/6000 Model 43P-140 gegen ein Doppelprozessorsystem des Typs RISC System/6000 Model 43P-240 unter dem Betriebssystem IBM AIX Version 4.2.1 Stand 98-04-06 ausgetauscht. Im Zuge dessen wurden sowohl systeminterne Features eingeführt (Security, Spiegelung der Root-Volume-Group) bzw. erweitert (separater, größerer Spool-Bereich) als auch Updates an den Software-Produkten (PD-Software wie elm, emacs, samba sendmail etc.) vorgenommen bzw. neu installiert (imap2, tin).

Erwin Srubar

NAG Fortran Library Mark 17

Auf den vom EDV-Zentrum betriebenen Servern `fpr.zserv, fbch, fe.zserv, la.zserv` und `fbma` steht die Version Mark 17 der NAG Fortran 77 Library zur Verfügung.

Die Bibliothek beinhaltet jetzt 1152 dokumentierte Unterprogramme. Wie schon bei der vorherigen Version fand auch diesmal wieder eine Erweiterung der Bibliothek um 43 Unterprogramme statt, davon wurden 10 Unterprogramme in das neue Kapitel F11 (*Sparse Linear Algebra*) aufgenommen.

Das Kapitel C06 (*Summation of Series*) wurde um ein Unterprogramm für eine komplexe 3D diskrete Fourier Transformation erweitert.

Um Unterprogramme mit neuen modernen Algorithmen wurden die Kapitel D02 (*Ordinary Differential Equations*), D03 (P*artial Differential Equations*) und E04 (*Minimizing and Maximizing a Function*) ergänzt.

In die Kapitel F02 (*Eigenvalues and Eigenvectors*) und F04 (*Simultaneous Linear Equations*) wurden 8 neue *black-box* Unterprogramme aufgenommen, denen Unterprogramme aus dem Kapitel F08 (LAPACK) zu Grunde liegen. LAPACK (*Linear Algebra Package*) ist eine Sammlung von state-of-the-art Algorithmen zur effizienten Lösung von Problemen der Linearen Algebra. Durch Implementierung eines Großteils dieser Algorithmen mit Hilfe von BLAS (*Basic Linear Algebra Subroutines*) Level 2 und Level 3 (Matrix*Vektor- und Matrix*Matrix-Operationen) werden beachtliche Performance-Verbesserungen erreicht.

Im Bereich der Statistik gibt es 13 neue Unterprogramme in den Kapiteln G02, G03, G04, G11, G12 und G13.

Informationen über diese Veränderungen beinhalten die Dateien `news` und `replaced` in dem Verzeichnis `/usr/local/nag/mk17/doc`.

Verwendung

Informationen über die Verwendung der Bibliothek enthält die Datei `readme` in dem Verzeichnis `/usr/local/nag/mk17` und auch die Manual Page

```
man   nag_fl_un          Users' Note.
```

Da die Hersteller der oben angeführten Rechner eigene Bibliotheken für BLAS-Routinen (SGI COMPLIB, DXML, AIX BLAS, ESSL, NEC BLAS) anbieten, stehen auf diesen Rechnern meist mehrere Versionen der NAG-Bibliothek zur Verfügung.

Ob man die NAG-BLAS-Routinen oder die hochoptimierten herstellerspezifischen BLAS-Routinen verwenden soll, kann durch Laufzeituntersuchungen entschieden werden. Beispiele dazu befinden sich auch in der Datei `readme`.

Auf dem Rechner `fbma` befindet sich eine Bibliotheksversion, bei der an die *'external-names'* ein *'underscore'* angefügt wurde, wie dies zur Verwendung von NAG-Unterprogrammen in anderen Programmpaketen verlangt wird (z. B. ACSL).

Als Hilfsmittel zur leichteren Verwendung der Bibliothek stehen Beispielprogramme (inkl. Eingabedaten und Ergebnissen) zur Verfügung, die auch als Vorlage zur Programmerstellung dienen können. Die dazu benötigten Dateien befinden sich in den entsprechenden Unterverzeichnissen von `/usr/local/nag/mk17/examples`.

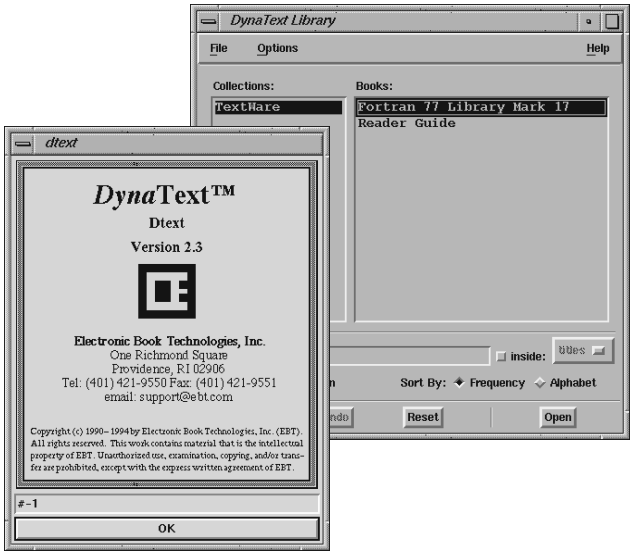
Es gibt eine Shellprozedur `nagexample` (mit dazugehöriger Manual-Page `man nagexample`) mit einem Parameter, der den Namen des Unterprogrammes angibt, dessen Beispielprogramm (inkl. dazugehöriger Daten, wenn notwendig) in das aktuelle Verzeichnis kopiert, übersetzt und anschließend auch ausgeführt wird.

Beispiel für die Verwendung des Beispielprogrammes zur Routine `a02aaf`:

```
nagexample a02aaf
```

Dokumentation

Außer auf der `la.zserv` gibt es eine Hypertext Online-Dokumentation (DynaText von Electronic Book Technologies, Inc.) mit dazugehörigem *Reader Guide*, die mit `dtext` aufgerufen wird (siehe Abbildung).



Das aus 12 Ordnern bestehende NAG FORTRAN Library Manual liegt bei mir im Zimmer (EDV-Zentrum, Wiedner Hauptstraße 8-10, 2. Stock, roter Bereich, DC02O14) zur Einsichtnahme auf.

Bei Schwierigkeiten mit den NAG-Produkten wenden Sie sich bitte an mich (Klappe 5492). Beachten Sie auch die entsprechenden WWW-Seiten `http://www.edvz.tuwien.ac.at/zserv/sw/nag.html`

Walter Haider

Organisatorische Neuerungen bei der Campussoftware

Die quartalsmäßigen Abrechnungen der Institutsunterstützung bezüglich der Kostenersätze für die Workstation-Wartung bzw. die Campussoftwarelizenz-Wartung werden in Zukunft in diesen beiden Bereichen getrennt erfolgen. Bisher waren diese beiden Bereiche auf einer Seite zusammengefaßt, obwohl sie unterschiedliche Service-Bereiche und Verrechnungsmechanismen repräsentieren. Außerdem werden wir im Laufe des Jahres die Kostenersätze auch in Euro ausweisen.

Die quartalsmäßigen Abrechnungen bzgl. der Campussoftware-Updatewartung der Campussoftwarelizenzen werden in Zukunft ebenfalls umgestellt:

Wurde bisher die Wartung jeweils ein Jahr im voraus bezahlt, so wird in Zukunft die Einheit der Wartungsintervalle auf ein Quartal reduziert und damit die Flexibilität erhöht. Sie bezahlen damit jedes angefangene Quartal und können in dieser Zeit die Softwareprodukte in allen Versionen und Sprachen vom Softwareserver beziehen. Im Quartal der Bestellung ist dieser Zugang in jedem Fall bis zum Quartalsende möglich, auch wenn Sie das Produkt ohne Wartung bestellen. In diesem Falle ist die Updatewartung im Einstiegspreis eingerechnet. Beachten Sie bitte, daß die Updatewartung zwar den Bezug der neuesten Softwareprodukte über den Softwareserver beinhaltet, aber keine Unterstützung durch die Institutsunterstützung oder die Herstellerfirmen.

Im Zusammenhang mit dieser Umstellung werden auch die Preise neu bemessen und zwar so, daß sich die Einstiegsgebühren und die Wartungsgebühren aliquot zu den alten Preisen darstellen, im allgemeinen werden die Wartungsgebühren ein Viertel der alten betragen. In jedem Fall entsteht für die Institute eine zeitweilige Entlastung, da die Vorschreibungen nicht mehr über einen Jahreszeitraum im voraus wirksam werden. Außerdem erhalten Sie so jedes Quartal eine Übersicht über Ihre gesamten gebuchten Softwarelizenzen.

Wie bereits erwähnt, können Sie die Wartung von Campussoftwarelizenzen auch beenden, in diesem Fall haben Sie aber w.o. erwähnt mit Ablauf des Quartals keinen Zugriff mehr auf den Softwareserver und auch kein lizenzmäßiges Recht mehr, die neueren Versionen einzusetzen. Diese Beendigung von Wartungsupdates können Sie jetzt auch online über WWW durchführen. Beachten Sie aber bitte, daß Sie bei einer neuerlichen Verwendung dieser Lizenzen wiederum die volle Einstiegsgebühr zahlen müssen. Damit soll verhindert werden, daß die Wartung nur dann gebucht wird, wenn man diese braucht oder gerade eine neue Release am Markt erscheint. Nur durch die breitflächige Nutzung dieser Wartungsmöglichkeit sind nämlich die Wartungsgebühren am Campus entsprechend günstig auszupreisen.

In Zukunft werden Campussoftwarelizenzen auch stornierbar sein, auch online über WWW. Das betrifft Lizenzen, die Sie nicht mehr brauchen und die Sie ab dem Zeitpunkt der Stornierung auch nicht mehr verwenden dürfen, weder in der gegenwärtigen noch in einer neueren Version. Dieses Stornieren ist durchaus sinnvoll, wenn Sie eine Lizenz nicht mehr benötigen, weil je nach Produkt diese Lizenzen dann anderen Bestellern weitergegeben werden können und damit eine bessere Effizienz der Lizenznutzungen im Rahmen der Verträge mit den Firmen erreicht werden kann. Es ist aber nach dem Urheberrecht und den Lizenzbestimmungen in keinem Fall gestattet, diese Lizenzen weiter einzusetzen, und wir ersuchen, diese Bestimmungen so wie bisher einzuhalten.

Informieren Sie sich bitte auch laufend im Web über unsere Campussoftware: `http://swd.tuwien.ac.at/css/` und wenden Sie sich in Fragen der Campussoftware an:

`campus@edvz.tuwien.ac.at`

oder direkt an die Sachbearbeiter.

Albert Blauensteiner

Neu bei campusweiter Software

Neue Produkte:

Adobe:

After Effects V3.1:
Erstellung von 2D-Animationen und Special Effects für Film, Video, Multimedia und Webprojekte

PhotoDeluxe V2.0:
Digitale Bildbearbeitung und Fotodesign

Plattformen: Windows 95/NT, Macintosh
Lizenzpreis: 375,-
Updatewartung/Quartal: 75,-

F-Secure SSH:
Das F-Secure SSH Terminal ermöglicht eine sichere Login-Verbindung über ein unsicheres Netzwerk. Das F-Secure SSH Terminal ist ein Ersatz für das Telnet-Protokoll. Das Terminal verwendet kryptographische Authentifikation, automatische „Session-Encryption“ und Methoden zur Sicherung der Integrität, die im SSH-Protokoll definiert sind.
Version 1.1 für Windows 3.x, Windows 95/NT
Version 1.0 für Macintosh
Version 1.3.3 für Unix
Lizenzpreis: 125,-
Updatewartung/Quartal: 25,-

Message Exchange:
Message Exchange (MX) der Firma Madgoat ist ein Mail Transport System für OpenVMS VAX und Alpha Systeme. MX umfaßt auch Features für das Verringern oder Beseitigen von Junk-Mails und kann Mail-Relaying kontrolliert unterbinden.
Version 5.0
Lizezpreis: 100,-
Updatewartung/Quartal: 25,-

Neue Produktversionen:

Claris:

Claris Home Page	Windows 95/NT	V2.0
ClarisWorks	Windows 95/NT	V5.0
FileMaker Pro	Windows 95/NT	V4.0
FileMaker Pro Server	Windows 95/NT	V3.0
Claris Home Page	Macintosh	V2.0v1
Claris Organizer	Macintosh	V2.0v2
ClarisWorks	Macintosh	V5.0v1
FileMaker Pro	Macintosh	V3.0v4
FileMaker Pro Server	Macintosh	V3.0v4

Corel:

CorelDRAW, engl.	Windows 95/NT	Version 8.0
WordPerfect Suite 8, engl.	Windows 95/NT	Version 8

eXceed:

PC	Windows 3.x	Version 5.2.1
PC	Windows 95/NT	Version 6.0.1

FrameMaker+SGML:

PC	Windows 95/NT	Version 5.5
Macintosh	MacOS	Version 5.5

FrameMaker:

WS	AIX, HP-UX, Irix, Solaris, SunOS	Version 5.5.3

HyperCard:

Macintosh	MacOS	Version 2.4

IDL:

PC	Windows 3.x,Windows 95/NT	Version 5.0.3
Macintosh	MacOS	Version 5.0.3
WS	Unix, OpenVMS	Version 5.0.3

IrfanView32:

PC	Windows 3.x,Windows 95/NT	Version 2.80

Mathematica:

PC	Linux, NeXTSTEP (Intel)	Version 3.0.2
WS	AIX, Dig UNIX, HP-UX, Irix, NeXT, Solaris, SunOS	Version 3.0.2

MacOS:

MacOS, dt.+engl.		Version 8.1

Maple V:

PC	Windows 95/NT, Linux	Release 5
Macintosh	MacOS	Release 5
WS	AIX, Dig UNIX, HP-UX, Irix, Solaris	Release 5

MATLAB:

MATLAB	Windows 95/NT	Version 5.2
Simulink	Windows 95/NT	Version 2.2

MICROGRAFX:

Windows DRAW	Windows 95/NT	Version 6

Microsoft:

BackOffice, dt+us		Version 4.0
DevNet	Windows 3.x,Windows 95/NT	April 1998
Exchange Server, dt+us	Windows NT	Version 5.5
Exchange Service Pack 1	Windows NT	Version 5.0
FrontPage 98, dt+us		Version 2.0
Office 97 Prof., dt.	Windows 95/NT	
Project 98, us	Windows 95+/NT	
Publisher 98, us	Windows 95+/NT	
TechNet	Windows 3.x,Windows 95/NT	Mai 1998
Windows 95 OSR2		
Windows 98 Candidate 0 (Beta)		

NAG Fortran77 Library:

DEC Alpha	Digital UNIX	Mark 18
HP9000/7xx, 8xx	HP-UX	Mark 18
SGI	Irix 5	Mark 18

NAG C Library:

PC	Linux	Mark 4

NAG TextWare für f77 Library:

WS	AIX, Digital UNIX, HP-UX, Irix 5, Solaris, SunOS	Mark 18

Norton:

AntiVirus, engl.	Windows 95/NT	Version 4.0
AntiVirus, dt.	Macintosh	Version 4.5.1
Commander, engl.	Windows 95	Version 1.0
Internet FastFind, dt.	Windows 95/NT	Version 1.0
pcANYWHERE, engl.	Windows 95/NT	Version 8.0
Utilities, dt.+engl.	Windows 95	Version 3.0
Utilities, dt.	Macintosh	Version 3.5.1
Utilities, engl.	Macintosh	Version 3.5

Oracle:

Oracle8 Server	AIX	Version 8.0.3.0.50
Oracle8 Server Patch	AIX	Version 8.0.3.2.1
WebServer	AIX	Version 2.1.1
Oracle8 Server	Digital UNIX	Version 8.0.3
WebServer	Digital UNIX	Version 2.1.0
Oracle8 Server	HP-UX	Version 8.0.3
Oracle8 Server Enterprise	HP-UX	Version 8.0.3.2
WebServer	HP-UX	Version 3.0
Oracle8 Server On-line Doku	Unix	Version 8.0.3

PC/TCP:

OnNet	DOS/Windows 3.x	Version 2.1
PC/TCP	DOS/Windows 3.x	Version 4.1

SigmaPlot:

PC	Windows 95/NT	Version 4.01

SPSS:

PC	Windows 95/NT	Version 8.0
Missing Value	Windows 95/NT	Version 7.5

VirusScan (McAfee):

PC (Vshield)	DOS	Version 3.1.4
PC	Windows 3.x	Version 3.1.4
PC	Windows 95	Version 3.1.4
PC	Windows NT	Version 3.0.3
PC	OS/2	Version 3.1.5
PC (Netshield)	Novell	Version 3.0.3
PC (Netshield)	Windows NT	Version 3.0.3

VirusUtilities:

PC	DOS, Windows, Windows 95, Windows NT WS + Server	Version 3.12A

Die Verteilung der campusweiten Software erfolgt fast ausschließlich über einen unserer Server. In ganz wenigen Fällen – wenn z. B. der Bedarf sehr gering ist – verleihen wir die Medien.

Alle Bestellformulare für die campusweite Software liegen im Sekretariat des EDV-Zentrums auf bzw. können auch dort telefonisch bestellt werden (Klappe 5485). Außerdem befinden sich alle Bestellformulare auch als PostScript bzw. PDF Files auf dem Server `swd.tuwien.ac.at` (Directory `info/BESTELLF`) bzw. auf dem WWW Server des Bereichs Institutsunterstützung (siehe weiter unten). Ferner haben Sie auch die Möglichkeit der online Bestellung über WWW (siehe `http://iuinfo.tuwien.ac.at/css/css.html`).

Alle relevanten Informationen über campusweite Software erhalten Sie auf dem WWW-Server des Bereichs Institutsunterstützung

```
http://iuinfo.tuwien.ac.at/css/css.html
```

oder mit FTP über den Softwareserver

```
ftp swd.tuwien.ac.at
userid:  campus
passwd:  tuwien
cd info
```

Ferner werden alle Neuigkeiten über campusweite Software in der Newsgroup **at.tuwien.edvz.neuigkeiten** gepostet.

Helmut Mayer

Systemunterstützung für AIX

Da die Kosten für die AIX-Systemsoftware im Vergleich zu den Campusverträgen anderer Plattformen günstig sind, freut es mich, die Reduktion der den Instituten rückverrechneten Wartungskosten bekanntgeben zu können:

Ab sofort werden die Wartungskosten für die AIX-Systemsoftware halbiert, das sind nun pro System 2,000.- Schilling jährlich. Die Mengenstaffelung bleibt natürlich weiterhin unverändert wirksam.

Diese Aktion gilt solange der AIX-Campusvertrag vergleichsweise günstig ist.

Seit 24. April 1998 ist **AIX Version 4.3.1** verfügbar. Die Lieferung dieser Version (zusammen mit den aktuellen Versionen der C- und Fortran-Compiler) steht unmittelbar bevor. Wenn alles rechtzeitig eintrifft, steht der campusweiten Verteilung im Sommer nichts mehr im Wege. In AIX 4.3.1 ist sendmail 8.8.8 bereits enthalten, somit wird es noch leichter, die Mail-Relay-Problematik in den Griff zu bekommen.

Aktuelle Hinweise zum AIX-Support sowie zur Plattform selbst findet man unter

`http://iuinfo.tuwien.ac.at/aix-support.html`

Bernhard Simon

Systemunterstützung für Digital UNIX

Der Installationsserver

Der Installationsserver `digital-unix.tuwien.ac.at` stellt allen im TUNET registrierten Alpha Maschinen über NFS im Verzeichnis `/campus` die wichtigsten DECcampus CDs zur Verfügung. Darüber hinaus wird via WWW die gesamte, in `/campus` verfügbare Dokumentation angeboten. Diese Dokumentation ist mit Glimpse indizert, sodaß gezielt nach Stichworten oder auch Phrasen gesucht werden kann.

Versionen

Die aktuelle Version von Digital UNIX ist 4.0D. Für das dritte Quartal 1998 ist die Version 5.0 angekündigt, wobei vorher noch 4.0E kommen soll.

Aktuelle Informationen sind unter
`http://digital-unix.tuwien.ac.at/`
oder über den Info Server der Institutsunterstützung
`http://iuinfo.tuwien.ac.at/`
verfügbar.

Gerhard Kircher

Campusweite Systemsoftware

http://iuinfo.tuwien.ac.at/pss/

Campusweite Applikationssoftware

http://iuinfo.tuwien.ac.at/css/

Softwaredirektinstallation über WWW

http://swd.tuwien.ac.at/

Freeware für AIX, Digital UNIX und ULTRIX

Seit der letzten Aufstellung vom Februar 1998 gab es folgende Änderungen:

Paket	Programm
elm	elm (2.4ME+40)
gcc	gcc (2.8.1)
libstdc++	libstdc++ (2.8.1.1)
mtools	mtools (3.8)
tin	tin (1.4-980514)
util	bash (2.02)
xpm	Xpm (3.4k)

Da das Programm tin früher Teil des elm-Pakets war, ab jetzt aber in einem eigenen Paket verteilt wird, ist beim Update folgende Reihenfolge zu beachten:

1. elm deinstallien
2. elm Paket löschen
3. elm+tin Pakete holen
4. elm+tin installieren

Das Paket libg++ ist obsolet und wurde daher entfernt.

Eine komplette Übersicht über das aktuelle Freeware Angebot ist als File `FW-TAB.ps` in den einzelnen Plattform-Bereichen

```
ftp://ftp.tuwien.ac.at/pub/pss/aix/pd/
ftp://ftp.tuwien.ac.at/pub/pss/axposf1/pd/
ftp://ftp.tuwien.ac.at/pub/pss/ultrix/pd/
```

zu finden.

Im Zusammenhang mit den Artikeln zum Thema Sicherheit möchte ich wieder daran erinnern, daß weitere Pakete für Programme wie sendmail (8.8.8), ssh (1.2.23) oder tcp_wrappers (7.6) vorbereitet sind, jedoch vorsichtshalber nicht im Public-Bereich liegen, da deren Installation zumeist mit einer systemspezifischen Konfiguration verbunden ist, die nicht automatisch abläuft. Diese Programme werden – mit Installationsunterstützung – auf Anfrage bereitgestellt.

Die Pakete apache (1.2.6) sowie samba (1.9.18p7) erfordern ebenfalls genauere Installations- und Konfigurationskenntnisse und werden deshalb auch nur auf diesem Weg verteilt.

Bernhard Simon

Novell-Unterstützung

- Die CDs der Beta-Version der **Netware 5** sind mittlerweile eingetroffen, für einen Test blieb bis dato allerdings wenig Zeit. Dies ist auch der Grund, warum unter dem angekündigten URL `http://novell.tuwien.ac.at/netware5.html` noch nichts zu finden ist (Bitte noch bis Ende Mai gedulden). Für Infos bezüglich der 5er gilt nach wie vor `http://www.novell.com/netware5/brochure.html`

- **Netware 3.2**: Diese Netware-Version wird uns im Rahmen des MLA-Vertrages nicht als Upgrade zur Verfügung stehen. Die Gründe hiefür möchte ich an dieser Stelle ganz kurz anführen:

  Der MLA-Vertrag in der derzeitigen Form wurde mit Erscheinen der Netware 4.00 nur für diese Schiene abgeschlossen. Da nach einigen Wochen selbst Novell zugeben mußte, daß die Version 4.00 „etwas instabil“ im Betrieb war, wurde vereinbart, bestehende Netware 3.1x-Lizenzen in den MLA aufzunehmen und auch zu warten. Die Zeiten der Versionen 4.00 und 4.01 sind (glücklicherweise) vorbei und es steht seit der Version 4.1 eine sehr stabile Netware zur Verfügung. Deshalb wurde bei der letzten Verlängerung des MLA (im Sommer 1997) darauf hingewiesen, daß die Wartung der bestehenden 3er-Lizenzen mit Sommer ’99 (Ende der Laufzeit des derzeitigen MLA) ausläuft.

  Aber abgesehen von dieser Juristerei: die Netware 3.2 ist eine Netware 3.12 mit sämtlichen Patches (incl. des Jahr2000-Patches) sowie eines grafischen SYSCON.

- **MERCURY:** Wer seinen Novell-Server auch als SMTP-Gateway (Mail-Server) mittels Mercury betreibt, möge im sowohl im eigenen als auch im Interesse der TU auf die Version 1.40 upgraden. Dies ist nämlich die erste Version, welche die missbräuchliche Verwendung als Mail-Relay unterbindet (Stichwort Spamming, Spam-Mails, ...). Sie finden die Version 1.40 von Mercury f. Netware auf `novell.tuwien.ac.at/mirror/pub/mercury` (und leider nicht auf dem hervorragenden `gd.tuwien.ac.at`; der Grund liegt in einer geänderten Vertriebsstrategie seitens Pegasus/ David Harris).

Noch Fragen? Sie erreichen mich entweder unter Tel. 504 14 31 / 15 bzw. via Mail unter `ast@novell.tuwien.ac.at`. Oder Sie schauen einfach am Server vorbei: `http://novell.tuwien.ac.at`, die Informationen werden dort immer mehr.

Andreas Astleitner

DECcampus-Software für OpenVMS Alpha und VAX

Mit der DECcampus Release AD01 Mar 98 stehen folgende CDs für OpenVMS Alpha und VAX zur Verfügung:

Beschreibung	Neu	Datum	Label
OpenVMS VAX Operating System V7.1 Bin.		Dec 1996	VAXVMS071
OpenVMS VAX Operating System V6.2 Bin.		May 1995	VAXVMS062
OpenVMS Op. System V7.1 On-Line Docu.		Dec 1996	OVMSDOC071
OpenVMS VAX Software Product Library	*	Dec 1997	VAXBINDEC97n
OpenVMS VAX Online Documentation Library	*	Dec 1997	VAXDOCDEC97n
OpenVMS Alpha Operating System V7.1 Bin.		Jan 1997	ALPHA071
OpenVMS Alpha Operating System V6.2-1H3		May 1996	ALPHA0621H3
OpenVMS Alpha Operating System V6.2 Bin.		Jun 1995	ALPHA062
OpenVMS Alpha Software Product Library	*	Mar 1998	AXPBINMAR98n
OpenVMS Alpha Online Documentation Lib.	*	Mar 1998	AXPDOCMAR98n
Alpha Systems Firmware Update V3.8		Dec 1996	UPDATE_V38
DIGITAL Enterprise Integration Server		Feb 1997	EISBINFEB97n
Enterprise Integration Server Docu.		Feb 1997	EISDOCFEB971
OpenVMS Management Tools f. Windows NT	*	Feb 1998	OMT030
DECcampus for OpenVMS	*	Mar 1998	VCAMPUSMAR81
DECevent Utility V2.2 for OpenVMS Alpha.		Aug 1996	DIA_V2_2
InfoServer V3.5 Kernel Software		Sep 1997	IS_V3.5
OpenVMS Freeware V3.0		Nov 1996	FREEWAREV30
OpenVMS Internet Product Suite V1.1		Nov 1996	OVMSIPS11
DIGITAL Firewall for OpenVMS V1.0		Jan 1997	OVMSIPS12
StorageWorks Media Robot Util V1.2,Mngmt		Jun 1997	—-

Interessante Neuigkeiten der letzten Release:

OpenVMS ALPHA

DEC C for OpenVMS Alpha....5.7
DISK$A2:[CC057]
DECprint Supervisor (DCPS) 1.4
DISK$A2:[DCPSAXP014]
Digital TCP/IP Services for....4.2
DISK$A3:[UCXAXP042]
Storage Library System for OpenVMS....2.9B
DISK$A6:[SLSB029]
Archive/Backup System for OpenVMS....2.2
DISK$A6:[ABS022]

OpenVMS VAX

DECprint Supervisor (DCPS) for 1.4
DISK$V1:[DCPSVAX014]
Storage Library System for OpenVMS....2.9A
DISK$V3:[SLS*029]

Windows NT

OpenVMS Management Tools für WNT....3.0
DISK$A0:[OMT030]

OpenVMS SW-Distribution-Service

Am VMS-Server EVAXSW sind folgende Distribution-CDs permanent online:

OpenVMS Alpha DISK$A1:, DISK$A2:, DISK$A3:, DISK$A4:

OpenVMS VAX DISK$V1:, DISK$V3:

OpenVMS Freeware V3.0 DISK$FREEWAREV30:

Internet Product Suite
DISK$OVMSIPS11:[INTERNET_PRODUCT_SUITE]

Teile der anderen Distribution-CDs sind auf EVAXSW::TU$KITS:[DECCAMPUS...] abgelegt. Die Distribution-Kits sind nur für eingetragene VMS-Systembetreuer (auch über DECnet Proxy-Access) zugreifbar, die Freeware- und die Internet Product Suite-CDs sind frei zugänglich.

Eine vollständige Liste aller DECcampus Software Produkte ist im File `gopher://evaxsw.tuwien.ac.at/00[DECCAMPUS]DECCAMPUS-CONTENTS.TXT` zu finden.

Diese und weitere Informationen zum OpenVMS-Support sowie zur Plattform selbst finden Sie über den Info-Server der Institutsunterstützung:

`iuinfo.tuwien.ac.at/vms-support.html`

Rudolf Sedlaczek

Betreuung MATLAB / ACSL

Seit 1995 betreut die Arbeitsgruppe ARGESIM die Softwarepakete MATLAB und ACSL durch:

- Verwaltung der Lizenzen
- WWW-Server-Gestaltung
- Organisation von Seminaren über Modellbildung und Simulation
- Update-Informationen
- Installations-Informationen
- Fachliche Beratung
- Vermitteln von Anwenderkontakten

Im folgenden die **Ansprechpartner**:

MATLAB und ACSL (Installation, fachlich, Vergleich):
Dr. F. Breitenecker (E114, Tel. 5374)

MATLAB (Installation, Vergleich):
M. Lingl (E114, Tel. 5386)

Installationsfragen (Workstations):
S. Wassertheurer (E114, Tel. 5419)

Lizenzserver:
P. Torzicky (EDV-Zentrum, Tel. 5494)

Campussoftware allgemein:
H. Mayer (EDV-Zentrum, Tel. 5603)

Campussoftware Lizenzen:
E. Schörg (EDV-Zentrum, Tel. 5482)

Email-Hotlines: `acsl@argesim.tuwien.ac.at`
`matlab@argesim.tuwien.ac.at`

News:

- MATLAB
  - Version 5.2 – PC, UNIX, MAC
  - Power System Toolbox für PC
  - Financial Toolbox für PC
  - Delzer Toolboxen für PC:
    CONTI, IDCON/ IDCON Nonlinear, MPA, ACD
  - Fuzzy Control Design (FCD) Toolbox, von system engineering GmbH Ilmenau
- ACSL 11.3 mit Security-Key (ohne Dongle) für PC

M. Lingl
ARGESIM / Abt. Simulationstechnik
Technische Universität Wien

Betreuung von CASe

Mit Beginn dieses Jahres hat die Arbeitsgruppe ARGESIM die inhaltliche und inhaltlich-organisatorische Betreuung der Computer Algebra Systeme (CASe) Mathematica, Maple und Derive übernommen. Sie wird folgende Angelegenheiten wahrnehmen:

- Update-Informationen
- Installations-Informationen
- WWW-Server-Betreuung
- Anwenderforum, Benutzerbetreuung
- Fachliche Beratung
- Organisation von Seminaren

Im folgenden die **Ansprechpartner**:

Mathematica, Maple, Derive (Vergleich, Organisation):
Dr. F. Breitenecker (E114, Tel. 5374)

Mathematica (fachlich):
Dr. G. Betz (E134, Tel. 5591)

Maple (fachlich):
Dr. W. Auzinger (E115, Tel. 5413)

Mathematica, Maple, Derive (Installation):
Ch. Almeder (E114, Tel. 5419)

Installationsfragen (Workstations):
S. Wassertheurer (E114, Tel. 5419)

Campussoftware allgemein:
H. Mayer (EDV-Zentrum, Tel. 5603)

Campussoftware Lizenzen:
E. Schörg (EDV-Zentrum, Tel. 5482)

Email-Hotline: `compalgs@argesim.tuwien.ac.at`

News:

- Maple V.5, alle Plattformen
- Testversion von „Maths & Fun“ für Mathematica auf Anfrage

M. Lingl
ARGESIM / Abt. Simulationstechnik
Technische Universität Wien

MATLAB · QUO · VADIS

EINE GESCHICHTE ...

8.30 Uhr. Herbert Labmater betritt sein Büro. Sein erster Griff – das Einschalten seines PC. Nach einem kurzen Blick in die Email und Erkennen der wesentlichen Mitteilungen durch jahrelange Übung (30% sofort löschen ohne Lesen, 30% löschen nach dem Lesen, 30% zur eventuellen Bearbeitung aufheben, 10% echt kognitiv erfassen) zeigt ihm der Terminkalender, daß für 9.00 Uhr eine Besprechung des Y10-Projektes geplant ist. Dafür muß Herbert Labmater noch eine Prinzipskizze für eine neue Gleichrichterschaltung vorbereiten. Kein Problem für Herbert Labmater, er verwendet die MWARE, und innerhalb Minuten hat er einen Leistungsgraphen skizziert und grob analysiert. Graphische Nachbearbeitung vertuscht noch etwas die doch geringe Vorbereitungszeit, denn in fünf Minuten beginnt das Meeting.

Vor dem Verlassen des Büros noch zwei Handgriffe, einmal der Griff zur Kaffeetasse, und einmal noch zum Keyboard: während des Meetings wird die MWARE eine Optimierung über den Gleichrichterentwurf fahren.

Die Sitzung läuft zufriedenstellend: der Entwurf und die Kenntnis des neuen Moduls kamen glänzend an (30 Minuten), des weiteren mußte ein etwas aufmüpfiger neuer Mitarbeiter erst davon überzeugt werden, doch die MWARE für seine Entwicklung zu verwenden (90 Minuten) – Herbert Labmater erinnert sich, früher ebenso rebellisch fadenscheinige Argumente gegen die MWARE verwendet zu haben.

11.00 Uhr. Herbert Labmater kehrt in sein Büro zurück. Nicht nur die Optimierung ist fertig, auch die Kaffeemaschine mit dem frischen Kaffee (leider übergeronnen). Es ist eine Espressomaschine, und befriedigt erinnert sich Herbert Labmater an die angebliche Auslegung der Funktion der Maschine – die MWARE hat unter Verwendung eines Modells mit partiellen Differentialgleichungen die optimale Dampfeinströmmenge berechnet – dieser Espresso muß einfach gut sein.

Die Entspannung nach dem Meeting läßt noch auf sich warten, nicht jedoch das Telefon: der Kollege aus der Schulungsgruppe für die MWARE ist krank, Herbert Labmater muß nachmittags die Einschulung der neuen Kollegen (größtenteils Hochschulabsolventen mit technisch-naturwissenschaftlichem Background bzw. äquivalente Ausbildung) in die MWARE übernehmen.

Kein Problem für Herbert Labmater (außer der Frage, warum schon wieder er): die MWARE erstellt durch die Notebookfunktion sozusagen selbst Lehrunterlagen, und das bis zur Mittagspause.

12.30 Uhr. Mittagspause. Herbert Labmater strebt der Kantine zu – und ist verblüfft. Kein langen Warteschlangen, kein Gedränge. Sein Gedächtnis schlägt zunächst im Terminkalender nach – auf der Suche nach einem vergessenen Fenstertag, bevor es die Antwort gibt: ab heute gilt ja die neue Essensordnung, bei der Abteilungen – abhängig von ihrer Größe, ihrer Entfernung am Betriebsgelände etc. unterschiedliche Essenszeiten haben – optimiert nach Zeit und Ort durch die MWARE (eine dankenswerte Leistung der Arbeitsgruppe Public Relations).

13.15 Uhr. Herbert Labmater kehrt daher früher in sein Büro zurück. Er hat noch Mittagspause und erinnert sich an eine unangenehme Sache: morgen soll er in seiner Arbeitsgruppe über eine neue Entwurfs- und Analysemethodik berichten, „Fuzzelsysteme“ oder so ähnlich. Er wirft die MWARE an, und vergräbt sich in die Verzeichnisse der nichtoffiziellen Teilmodule.

Sein Ziel ist der Modul, der ihm – alle Gegebenheiten in Betracht ziehend und seine Zulagen optimierend – aussagt, ob er morgen noch gleitzeiten kann, oder ob ein taktischer Arztbesuch noch sinnvoller wäre – womit der leidige Vortrag zwar nicht aufgehoben, aber aufgeschoben wäre. Auf dieser Suche stößt Herbert Labmater auf die (natürlich) HTML-unterstützte Einführung und Bedienung eines „Fuzzy System“ Teilmodul. Er lehnt sich zufrieden zurück, der Vortrag morgen ist gerettet, kein Problem mehr für Herbert Labmater.

14.09 Uhr. Krise: Herbert Labmaters Tochter hat angerufen. Die Mathematikschularbeit ist vorverlegt worden. Er muß die für das Wochenende versprochenen Lösungen der Vorbereitungsbeispiele noch heute liefern. Herbert Labmater erinnert sich mit Widerwillen an das Buch in seinem Aktenkoffer: „Mathematik für die Oberstufe“. Dieses Buch sollte ihm die Lösungen ermöglichen und sein Gesicht in der Familie wahren helfen (*ein Entwicklungsingenieur wird doch die paar Integrale lösen können !*).

Herbert Labmater ist nicht umsonst dabei, in die Managementebene aufzusteigen: er probiert Krisenbewältigung nach dem Delegationsprinzip. Er will einer Kollegin, der die Fama die Fähigkeit zur analytischen Berechnung von Integralen nachsagt und die zumindest bis gestern dringend eine zeitliche Analyse des Dining Philosophers'-Problem suchte, ein Tauschgeschäft vorschlagen: Berechnung der Integrale gegen einen Tip zur Berechnung des Dining Philosophers'-Problems. Herbert Labmater will ihr Petrinetze als Beschreibungsform vorschlagen, und als Implementierungs- und Analysewerkzeug die State Machine der MWARE anraten, von der nur er zu wissen glaubt, da diese erst gestern mit der neuen Release der MWARE (die erst vierte in diesem Monat) kam. Die Enttäuschung folgt auf dem Fuße: die Kollegin gehört zur δ-Testgruppe der MWARE und weiß schon lang von der State Machine, und hat sie gestern abend mit Erfolg auf ihr Problem angewendet.

Glücklicherweise ist die Kollegin eine echte Kollegin und noch nicht im Management, sie gibt einen heißen Tip ohne Gegenleistung: ein Modul der MWARE. Nach kurzer Suche findet sich der Symbolic Modul der MWARE, und in 30 Minuten sind alle neunzehn Integrale gelöst, und darüber hinaus noch fein säuberlich gemalt – kein Problem mehr für Herbert Labmater.

15.03 Uhr. Der Einführungskurs in die MWARE ist von ausgesprochener Langweiligkeit. Nicht, daß die Materie uninteressant wäre, die neuen Kollegen lernen mit der MWARE programmieren, sie lernen technische Berechnungen ansetzen und analysieren, sie lernen begleitende betriebswirtschaftliche Kalkulationen durchzuführen und zu dokumentieren und dabei zu beschönen, aber heute ist es besonders öd, fast alle Teilnehmer scheinen zu schlafen.

Herbert Labmater erinnert sich an vergangenes Jahr, wo er zufällig denselben Teil der MWARE vorzutragen hatte, und an das vorvergangene Jahr, wo er selbiges noch als Mitglied der MWARE-Ausbildungscrew tat: voriges Jahr hatte wenigstens die Hälfte der Teilnehmer Interesse gezeigt, ein Viertel selbiges geheuchelt, und nur der Rest hatte geschlafen. Vor zwei Jahren war es noch besser: fast alle hatten nicht geschlafen, denn von einer Beherrschung der MWARE hängt der Aufstieg in der Firma ab.

Herbert Labmater will der Sache auf den Grund gehen: er synchronisiert seine Bedürfnisse mit dem eines Teilnehmers und hat daher Gelegenheit, diesen vor der Tür nach dem Grund der allgemeinen Fadesse und Tristesse zu fragen. Die Antwort zeigt Herbert Labmater, wie richtig es war, die MWARE-Schulungsabteilung zu verlassen: fast alle Teilnehmer haben während ihrer Hochschulausbildung bzw. sonstigen Ausbildung die MWARE zumindest kennengelernt, und viele haben mit ihr ihre Diplomarbeit oder noch Ärgeres gemeistert.

Herbert Labmater tut das einzig Richtige: er verabschiedet die Teilnehmer mit „Sie wissen alle schon sehr viel über die MWARE, wir machen morgen weiter“ und fügt in Gedanken hinzu „dann kann sich ein anderer Kursleiter fadisieren und frustrieren“.

16.15 Uhr. Beinahe schon Büroschluß, der Tag scheint friedlich auszuklingen. Herbert Labmater bereitet sich bereits geistig auf seine Beschäftigung nach Büroschluß vor (Stichwort Carrera), als ihn ein zwar privater, aber sehr unheildrohender Anruf aus dieser angenehmen Beschäftigung reißt. Am Telefon ist die gute alte Tante (und Erbtante) Margarete. Sie ist aufgeregt: der Berater in ihrer Bank hat dringend zu einer Umstellung der Anlagen geraten, besonders wichtig sei der rascheste Ankauf bestimmter Aktien, die nur mehr kurzfristigst zu erhalten seien und die einen guten Gewinn versprächen.

Herbert Labmater ist ein Mann schneller Entschlüsse: bevor er sich mit der Tante in endlosen Diskussionen ergeht, läßt er sich von ihr die Eckdaten dieses hochgepriesenen Angebots per Fax schicken und verspricht noch vor Bankschluß eine Antwort.

Aber wie ? – kein Problem für Herbert Labmater. Er versteht zwar wenig bis gar nichts von Anlagenbewertung, Portfolios und Ähnlichem, aber die MWARE hat auch einen finanzmathematischen Modul für Laien.

Fünf Minuten vor 17.00 Uhr ist die Angelegenheit mit einem Anruf bei der Tante und mit einem Anruf bei der Bank – mit der dringenden Empfehlung, die Tante eher bei der Umstellung auf den Euro denn bei der Veranlagung ihrer Gelder zu beraten, erledigt, und um 17.00 Uhr kann Herbert Labmater die Mühen des Bürotages beenden.

Die letzte Tätigkeit Herbert Labmaters im Büro: er beendet mit einem dankbarer Blick auf das MWARE-Logo die MWARE, die natürlich im Autostart steht und sich nun auch eine Ruhepause verdient hat.

17.30 Uhr. Herbert Labmater trifft zu Hause ein, und übergibt seiner Tochter als erstes die Lösungen der Integrale. Dann zieht er sich in seine Garage zurück, denn er hat noch besonderes vor: als Obmann des Carrera-Modell-Racingclubs ist er seinem Verein zur Generalversammlung etwas besonderes schuldig: er wird einen Modellwagen mit einem Mikroprozessor ausrüsten, der mit einer intelligenten Steuerung dem Lichtsignal eines vor ihm auf der Nebenbahn fahrenden Wagens folgen und dabei alle Beschleunigungs- und Bremsmanöver mitmachen wird – auch das erledigt die MWARE (natürlich auch zu Hause auf allen Rechnern installiert) für Herbert Labmater, aber das ist eine andere Geschichte.

22.17 Uhr. Herbert Labmater hat den Prototyp des Verfolgewagens zum Laufen gebracht, er entspannt sich in seinem Arbeitszimmer, und am Computer geht er seinem geheimsten Hobby nach, dem Betrachten der Schönheit der Mathematik: Die MWARE berechnet und zeigt ihm die schönsten Fraktale. Das braucht seine Zeit, denn gut Ding braucht Weile, vor allem die MWARE, und Herbert Labmater kann Gedanken zu diesem ereignisreichen Tag seinem Tagebuch anvertrauen*: Dir mein liebes Tagebuch, höchst vertraulich:* MWARE *hat mir heute den Tag gerettet, verschönt, versüßt – wie habe ich früher ohne* MWARE *arbeiten, leben, sein können – auch du kannst mir darüber keine Auskünfte geben – und wie sieht eine Zukunft ohne* MWARE *aus – wenn die Lizenzen unbezahlbar werden, das Chaos ?,* und dann wieder prosaischer (Herbert Labmater leistet sich nur selten derartige barocke philosophische nicht ernstzunehmende verbale Ausschweifungen): *und übrigens wirst du, liebes Tagebuch, nächste Woche durch ein* MWARE *Notebook ersetzt.*

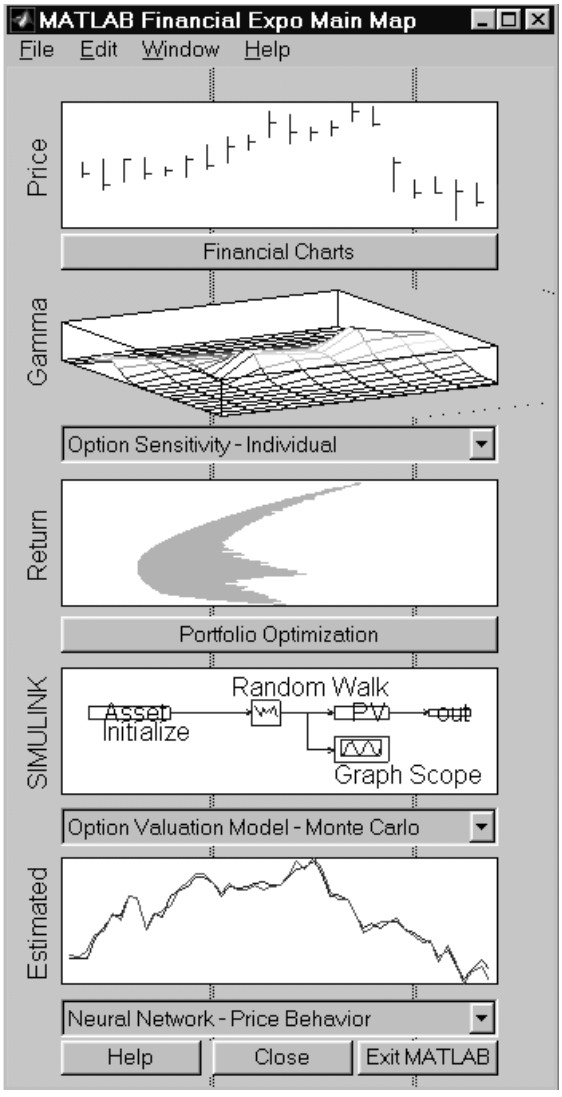
Das Fraktal erscheint, die Faszination wird allerdings durch einen kleinen Zettel, an den Bildschirmrand geklebt, beeinträchtigt. Herbert Labmater liest mit Stirnrunzeln: *Internet war heute den ganzen Tag belegt, bitte am Abend nochmals die Homepage der* MWARE *kontaktieren und drei Mousepads, sechs Kaffehäferl, und drei T-Shirts (S, M und XXL) mit dem Aufdruck* MWARE*, die farbige Version, bestellen; danke übrigens für Zahlung mit deiner Kreditkarte.*

Gedankenverloren tippt Herbert Labmater ein `http://www.mathworks.com`, bevor ihm die Augen zufallen. Sein letzte Wahrnehmung vor dem Schlaf ist das blinkende MWARE-Logo:

FAKTEN

Ist, wird MATLAB die MWARE ? Vor etwa zwei Jahren konnte noch zusammengefaßt werden, daß MATLAB ein sehr guter Interpreter für Matrix- und Vektoroperationen ist, und durch die vielen Toolboxen auch ein sehr weites Anwendungsspektrum hat, aber als „Universalmittel für Alles“ nur die zweitbeste Lösung in der Mehrzahl der Aufgaben ist. In den letzten zwei Jahren allerdings hat MATLAB in vielen Bereichen den ersten Platz übernommen, und manche Konkurrenzprodukte führen einen verzweifelten Abwehrkampf.

MATLAB hat derzeit auf drei neuen Fronten die Mitbewerber gehörig in die Zange genommen: im Anwendungsbereich der Finanzmathematik, im Bereich der Zustandsgraphenbeschreibung und -Analyse und im Bereich der graphischen Modellbildung kontinuierlicher Prozesse.



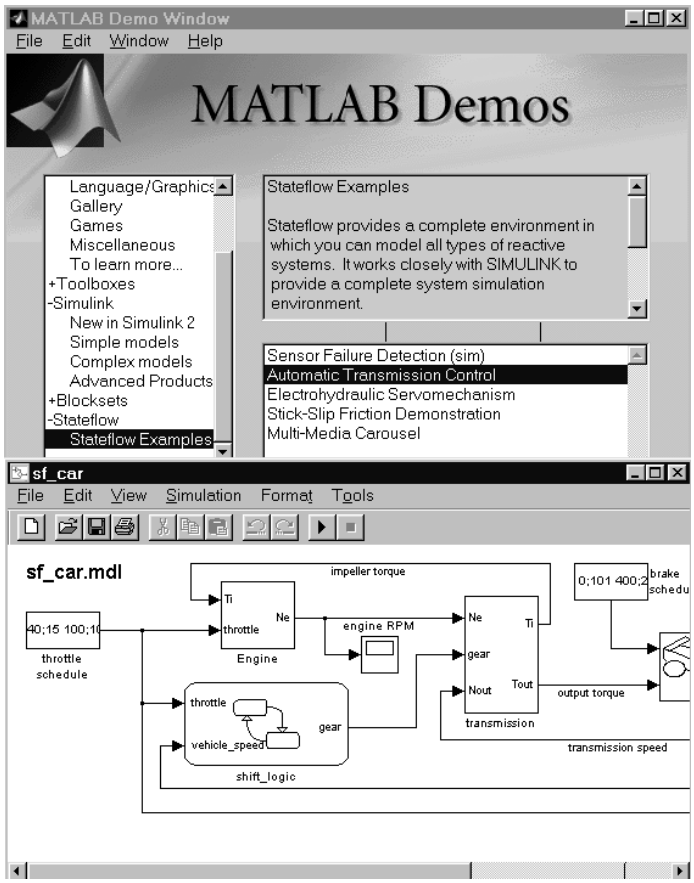
MATLAB hat mit seiner Financial Toolbox den Einstieg in die Finanzmathematik versucht, angekündigt im **MATLAB Universe** im Jahr 1995.

Der Einstieg den Finanzbereich sowie der Begriff des **MATLAB Universe** ist anfangs belächelt worden. Die Leistungen der Financial Toolbox (siehe obige Abbildung) sind zwar gediegen, aber dennoch erreichen sie nicht den Umfang und vor allem die Bequemlichkeit von eingesessenen Werkzeugen.

Mathworks verweist zwar noch auf Features der Statistik Toolbox und der Neural Network Toolbox, geht aber dennoch andere Wege, nämlich den der Zusammenarbeit mit Analysefirmen wie J. P. Morgan im Rahmen des Programms „Partners and Colleagues“. J. P. Morgan wird z.B. die MATLAB Engine als Basis seiner neuen Version des Value-at-Risk-Programms verwenden.

Wesentliche und essentielle Erweiterungen hat gemeinsam mit MATLAB 5 auch SIMULINK 2 erfahren, indem die klassische regelungstechnisch orientierte graphische Modellbeschreibung nun wesentlich erweitert wurde:

- durch Einbindung der Zustandsgraphenbeschreibung
- und durch die Erweiterung auf eine allgemeine nichtkausale graphische Modellbeschreibung.



Stateflow, die Zustandsmaschine von MATLAB (siehe obige Abbildung) ist wie SIMULINK mehr als eine Toolbox. Mit Stateflow können Zustandsautomaten und komplexe logische Zusammenhänge dynamisch beschrieben werden. Stateflow wurde auf Druck der Industrie eingeführt, als dynamische Alternative zu Statemate. Erwähnt sei, daß auch $MATRIX_X$ mit BetterState einen derartigen Modul entwickelt hat.

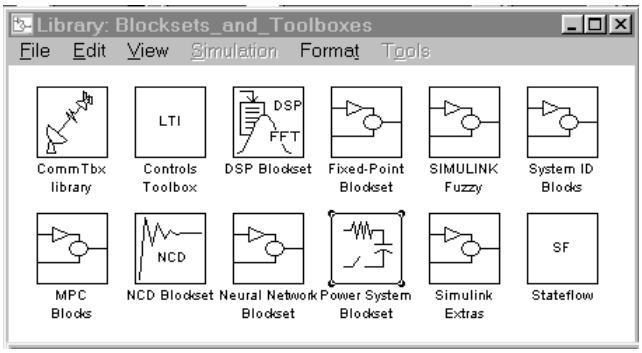
Betrachtet man die Stateflow-Dokumentation sowie die Beispiele in der MATLAB Demo (siehe obige Abbildung), so fällt ein beschränkter und relativ einfacher Einsatz auf.

Es scheint, daß für Mathworks selbst die Möglichkeiten von Stateflow überraschend sind, von der Steuerung

hybrider Modelle bis zur diskreten Simulation. Insbesondere bei rekursiven Graphen entstehen sehr komplexe Strukturen. Stateflow wird noch manche Überraschung bringen.

Mit Stateflow geht Mathworks auch in den Bereich der klassischen technischen Planung, und Stateflow zielt eindeutig in Richtung von Statemate, das in der Industrie sehr weit verbreitet ist.

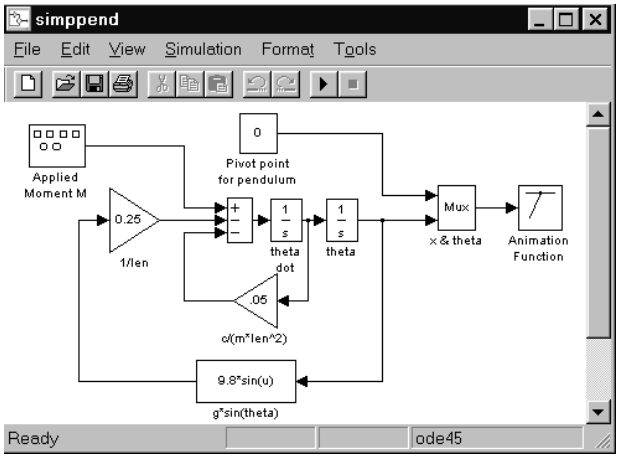
Ein Blick in die SIMULINK Library zeigt die Vielzahl der Blocksets und der Erweiterungen, u.a. auch Stateflow und das im folgenden beschriebene Power System Blockset:



Die dritte wesentliche Entwicklung besteht im „Aufbrechen“ der klassischen regelungstechnisch orientierten graphischen Modellbeschreibung in SIMULINK. Eine Verbindung zwischen zwei Blöcken ist in der klassischen Beschreibung ein eindeutig gerichtetes zeitabhängiges Signal *k(t)*, mit wohldefinierten Eingängen und Ausgängen, Rückkoppelungen müssen über Integrierer oder andere Memory-Blöcke gehen (siehe folgende Abbildung), um algebraische Schleifen zu verhindern und bei der Analyse den Aufbau der Zustandsraumbeschreibung

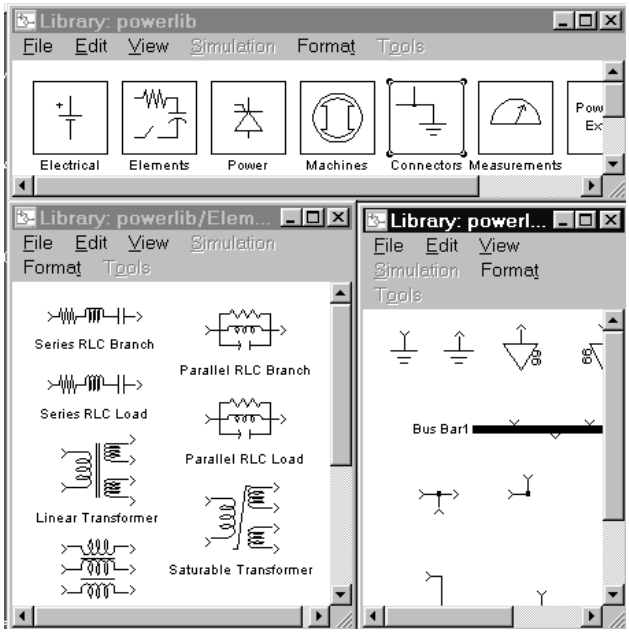
$$\dot{\vec{x}}(t) = \vec{f}(\vec{x},\vec{u},t), \quad \vec{y} = \vec{g}(\vec{x},\vec{u},t)$$

in Form einer s-function zu ermöglichen.

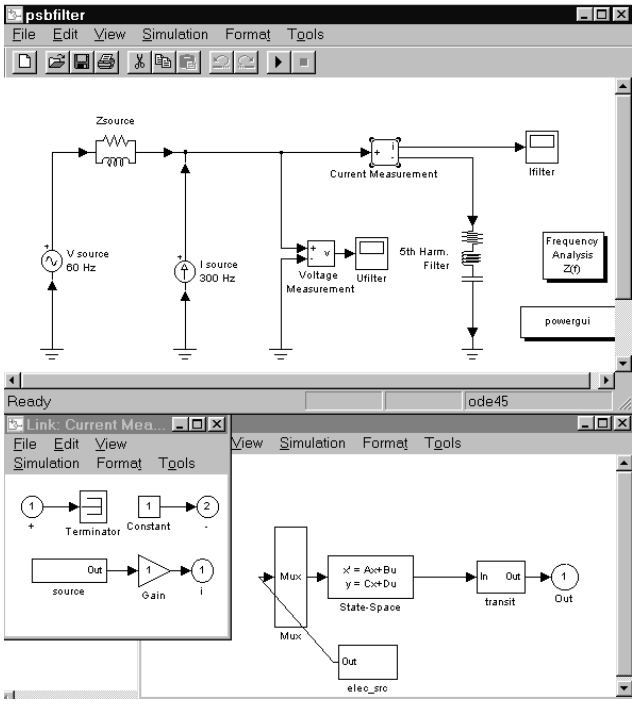


Die erste Erweiterung besteht in Verbindungen zu / in getriggerten bzw. enable- oder disable-fähigen Teilmodellen, wodurch die graphische Modellbeschreibung auch rein sequentiellen Code formulieren kann.

Der wesentliche Schritt wurde allerdings mit der Leistungsgraphen-orientierten Beschreibung im neuen Power System Blockset getan. Die Verbindungen sind nicht mehr kausale Signale, sondern Leistungsflüsse, aus denen die Modellbeschreibung in Zustandsform erst ermittelt werden muß. Die folgende Abbildung zeigt einen Ausschnitt aus der Library *powerlib*.



Ein Modell wird aus der Power System Toolbox aufgebaut, ein Blick hinter die Blöcke durch Unmasking z.B. des Blockes „Current Measurement“ zeigt größtenteils reines Handling von Input- und Outputrelationen (folgende Abbildung, links unten).



Im Prinzip sind die Measurement-Blöcke jene, in denen z. B. nach den Kirchhoffschen Regeln dann das klassische Modell abgeleitet wird.

Die Funktionsweise der Blöcke ist in ihrem Funktionsnamen verborgen und wird erst bei Aktivierung des Mo-

dells relevant: beim ersten Aufruf einer Simulation wird das SIMULINK Modell erst erzeugt, wie die Meldung

```
Power System Blockset Version 1.0 processing
psbfilter ...
Computing state-space representation of linear
electrical circuit...
(3 states ; 2 inputs ; 2 outputs)
Simulink equivalent state-space system stored in
block: psbfilter/Current Measurement
Ready for simulation
```

im MATLAB Command Window zeigt.

Das Modell wird dabei im Prinzip auf eine lineare Zustandsraumdarstellung abgebildet, die in den Block „Source“ gespeichert wird (vorhergehende Abbildung, rechts unten: Öffnen des Blockes „source“ im Block „Current Measurement“).

Mit dem Power System Blockset stellt MATLAB ein Werkzeug für die Entwicklung im Bereich der Leistungselektronik zur Verfügung MATLABs Zielrichtung ist damit u. A. SPICE.

Angekündigt als Third-Party-Produkt ist bereits ein Mechanic Blockset, das Leistungsgraphen-ähnliche Beschreibungsformen im mechanischen Bereich anbietet. Damit geht MATLAB auch in den Bereich der mechanischen bzw. mechatronischen Simulatoren wie SIMPACK, Mesa Verde etc.

Bei Toolboxen scheint sich MATLAB generell auf eher methodische Kernbereiche zurückzuziehen, während spezialisiertere Anwendungen den Third-Party-Produkten überlassen werden. Nur mehr selten werden derartige Third-Party Toolboxen auch über Mathworks vertrieben (wie die PDE Toolbox).

Insbesondere im deutschsprachigen Bereich finden Third-Party-Entwicklungen im Echtzeitbereich statt (Fa. dSPACE), und Third-Party Toolboxen der Firma Delzer stellen Werkzeuge für Microcontroller-Design und Identifizierung mit kontinuierlichen Strecken zur Verfügung.

Fast wöchentlich wird allerdings auch die Liste der Toolboxen- bzw. Module-erzeugenden Firmen länger (siehe Mathworks-Server).

Es scheint tatsächlich so zu sein, daß uns das **MATLAB Universe** Wirklichkeit wird, und Mathworks wird gut daran tun, mit dem beginnenden Monopol sehr vorsichtig umzugehen.

KRITIK UND SCHWACHSTELLEN ...

Ein Monopol ist prinzipiell schlecht, und eine Monopolstellung verdirbt den besten Charakter.

Das Gewicht von Mathworks bei Intel und Microsoft ist nicht zu vernachlässigen (Zusammenarbeit beim Pentium-Bug, Fehler bei der Notebook-Funktion unter Office 97 – wo Mathworks auf Nachbesserung durch Microsoft wartet und nicht vice versa).

Die Schwachstellen in MATLAB / SIMULINK sind einerseits hausgemacht: Probleme mit neuen Versionen, Inkompatibilitäten etc. Mathworks entwickelt teilweise zu rasch, rascher als es Vertrieb, Dokumentation und Anwender verkraften.

Essentielle Schwachstellen allerdings sind immer noch vorhanden – hier hat MATLAB / SIMULINK noch einen weiten Weg zur Nummer Eins. Einige sind:

- Probleme mit der Performance, insbesondere bei SIMULINK Modellen, wo die Simulationen teilweise sehr langsam werden. Hier spielt auch das noch nicht funktionierende Zusammenspiel zwischen Realtime Workshop und MATLAB Compiler eine Rolle.

- Genauigkeitsprobleme: Sind 16 signifikante Stellen wirklich genug ? – für den Großteil der Aufgaben sicher, aber für spezielle komplexe Aufgabenstellungen sind höhere Genauigkeiten wünschenswert. MATLAB verweist dabei auf die Symbolic Toolbox (den Maple Kern), in der theoretisch mit beliebig vielen signifikanten Stellen gerechnet werden kann – aber das Interface ist aufgrund der unterschiedlichen Philosophie problematisch.

- Verzicht auf jegliche Parallelisierung, auf jeder Ebene (vom Code in der Library bis zu m-Files). Mathworks leistet es sich sogar, Artikel wie „Why no parallelization in MATLAB“ zu publizieren.

- SIMULINK möchte nicht nur Nummer Eins bei den Simulatoren sein, es möchte auch alle Bereiche abdecken. Nach wie vor fehlt aber eine effektive Behandlung impliziter Modelle, wie sie u. A. in der Mechanik vorkommen. Hier ist noch prinzipielle Arbeit an den s-functions notwendig.

- Ein interessanter Punkt ist das Fehlen von Mathworks Toolboxen zur Identifizierung mit kontinuierlichen Modellen – alle Toolboxen sind auf die Identifikation mit diskreten Modellen ausgerichtet – was u. A. eine Verwendung der Modelle in SIMULINK einschränkt. Hier springt Delzer hilfreich mit den IDCON-Toolboxen ein.

UND AN DER TU WIEN ...

Wurde Herbert Labmater an der TU Wien ausgebildet – oder bekommt er demnächst eine Stelle an der TU Wien ? Kaum, wohl eher werden wir gewollt oder ungewollt zu Herbert Labmater – denn es sind alle Toolboxen, auch Third-Party Toolboxen verfügbar, Projekte werden in MATLAB durchgeführt etc.

Einerseits ist es gut, wenn eine Arbeitsumgebung international anerkannt ist, den Austausch erleichtert etc. – aber dennoch ist eine kritische Betrachtung sinnvoll.

In diesem Zusammenhang ist es bemerkenswert, daß beim MATLAB-Seminar im März dieses Jahres viel weniger kritische Stimmen zu hören waren als beim Seminar im Vorjahr – sind wir wirklich so zufrieden ?

Prof. Dr. F. Breitenecker
Abt. Simulationstechnik
Inst. f. Technische Mathematik

INSTRUMENTUM · UNIVERSALE · MATLAB · ERIT · IN · ORBE · TECHNICO · PRIMUM · SECUNDUM · TERTIUM · ET · ULTIMUM.

Die SIDES Authorisierungsinfrastruktur für die TU Wien

Der eine hat's, der andere braucht's.
Man muß drauf schau'n, daß es der, der's braucht, kriegt,
wenn er's will und beide dabei glücklich sind.

Beschreibung einer personenbezogenen rollenbasierten Zugriffskontrolle und dezentralen Rechteverwaltung – SIDES Sicherheit für Resourcen im WorldWideWeb.

Stellen Sie sich vor, Sie möchten sich von Ihrem Freund, dem Franz, einem wahren Kenner klassischer Musik übrigens, die Goldberg-Variationen von Bach, natürlich in der Interpretation Glenn Goulds, ausborgen. Sie rufen ihn also an und fragen, ob er Ihnen die Platte borgt. „Aber ja", meint er, „ich kenn dich ja, du paßt mir sicher gut d'rauf auf und wenn ich sie wieder brauch' krieg' ich sie eh gleich wieder, nicht wahr?" „Natürlich", versichern Sie, und Franz schlägt vor, Ihnen die Platte vorbeizubringen, dann könne er sich nämlich auch gleich Ihren neuen Pentium II Computer ansehen. Das mit der Schallplatte wäre also geregelt ...

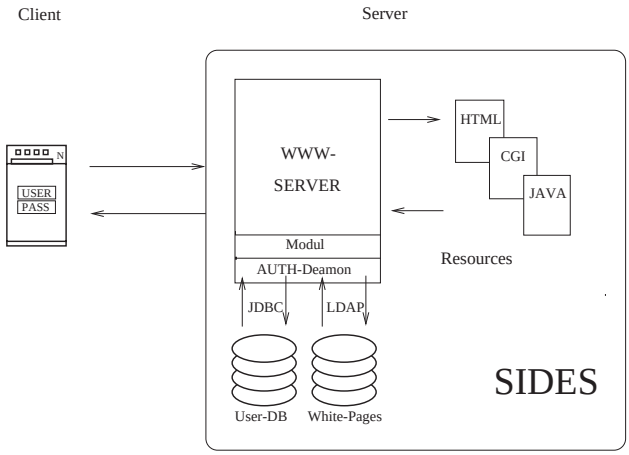
Und wie ist das nun, wenn Sie (vielleicht mit Ihrem neuen Pentium II ?) auf eine Seite im Intranet zugreifen wollen? Sagen wir, auf eine Seite, oder gleich exakt formuliert, eine „Resource", die durch das Sicherheitssystem des Sicheren Internetbasierten DatenErfassungssystemes SIDES geschützt ist?

Identifikation

Zunächst müssen Sie „bekannt" sein, das heißt, Sie müssen über einen Eintrag in den White Pages der TU Wien verfügen. Das Personal der TU Wien wird regelmäßig (i.a. am Beginn des Monats) aus den Daten der Universitätsdirektion automatisch eingetragen, ebenso jene Studierenden, die im Rahmen des Mail/News/Info Services eine Berechtigung erhalten haben. An den Instituten können, von den jeweils zuständigen Address-Managern, zusätzliche Angehörige des Institutes hinzugefügt werden, beispielsweise jene, die privatrechtlich angestellt sind, oder jene, die über Drittmittel refundiert werden. Zu jedem White Pages Eintrag wird ein Paßwort vergeben.

Authentifikation

Im Weiteren geht es darum, Ihre Identität zweifelsfrei festzustellen. Im persönlichen Kontakt ist das relativ einfach: Franz erkannte Sie an Ihrer Stimme, Ihrer Art zu sprechen. In einem elektronischen System bedarf es naturgemäß anderer Merkmale. SIDES verwendet für die webbasierte Zugriffskontrolle eine sogenannte Basic Authentication: als Merkmale werden Benutzername und Paßwort herangezogen. Benutzername ist Ihr Nachname, als Paßwort wird jenes der White Pages verwendet. Die Eindeutigkeit folgt aus der Kombination beider Merkmale. Falls Sie beispielsweise Schmidt heißen, lassen Sie sich also bitte nicht davon irritieren, daß es mehrere Schmidts gibt. Benutzername ist in jedem Fall nur Ihr Nachname, Groß- und Kleinschreibung spielen dabei keine Rolle (*case insensitive*).



Sollte es im Anschluß an die Aufforderung zur Eingabe von „User Name" und „Password" zu einer Fehlermeldung kommen, gibt es dafür verschiedene mögliche Ursachen:

- Sie haben sich vertippt. Probieren Sie es bitte noch einmal.
- Das Paßwort ist vielleicht falsch. Sollten Sie es vergessen haben oder noch gar kein Paßwort haben, wenden Sie sich bitte an Ihren Address Manager.
- Die SIDES Authentifikation ist im Moment nicht verfügbar (weil zum Beispiel das White Pages Service der TU Wien nicht verfügbar ist). Über die Status-Seite (`http://www.lzk.ac.at/sides/status`) können Sie nachprüfen, ob dies der Fall ist.

Ist die Authentifikation erfolgreich, tritt das SIDES Sicherheitssystem im Normalfall nicht mehr sichtbar in Erscheinung. Das System zeichnet sich durch diesen einfachen Zugang aus: Sie brauchen sich kein neues Paßwort zu merken, weil jenes der White Pages Verwendung findet, und Sie müssen sich nur ein einziges Mal mit Nachname und Paßwort anmelden. Umgekehrt gewinnt damit das Paßwort an Bedeutung. Bitte wählen Sie es sorgfältig (keine einfachen Zeichenkombinationen) und ändern Sie es auch regelmäßig. Zur Änderung steht Ihnen das WWW Gateway der White Pages (`http://wp.tuwien.ac.at`) zur Verfügung.

Der nächste Schritt, die Überprüfung, ob Sie die gewünschte Resource auch „haben" dürfen, läuft in der Regel ab, ohne daß Sie es bemerken.

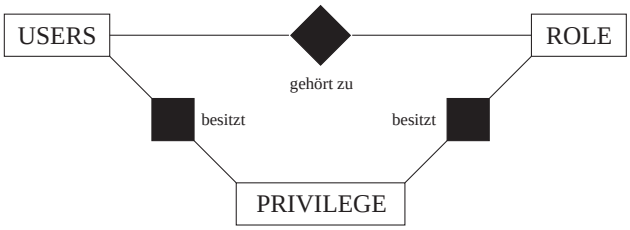
Authorisierung

Sie erinnern sich: Franz borgt seine Platten nur jenen Freunden, von denen er weiß, daß sie darauf aufpassen. Verschiedene Personen besitzen verschiedene Rechte. So verhält es sich auch in SIDES.

Für die Verteilung von Zugriffsrechten gibt es die Möglichkeit der automatisierten Rechtevergabe nach einem bestimmten Schema und der händischen Zuteilung an bestimmte Benutzerinnen und Benutzer.

Das bei der SIDES Authorisierung verwendete Schema ist eine

Rollenbasierte Rechteverteilung



Zunächst werden, abgeleitet aus Funktionen in der universitären Struktur, sogenannte Rollen (roles) definiert. Als Beispiel dafür lassen sich „Mitarbeiter eines Institutes“, „Lehrveranstaltungsmitwirkende“, „Institutsvorstände“ oder „Abteilungsleiter“ anführen. Diesen Rollen werden bestimmte Rechte (privileges) und Möglichkeiten zur Verwaltung von Rechten (grant privileges) übergeben. Schließlich werden Benutzern (user) Rollen zugeordnet. Damit verfügen die Benutzer über die den Rollen zugehörigen Rechte.

Die für die Zuordnung Benutzer/Rollen erforderlichen Informationen werden aus den Daten der Universitätsdirektion (TUWIS; Funktion, Zuordnung zu einem Institut) bzw. den Einträgen in den White Pages (Zuordnung zu einem Institut) gewonnen. Nachdem der Import dieser Daten jeweils einmal pro Woche erfolgt, wird die aktuelle Funktionsstruktur der Universität in den Zugriffsrechten widergespiegelt.

Rechte werden auch zentral seitens der SIDES Systemadministration händisch an bestimmte Personen vergeben. Insbesondere werden solcherart die sogenannten SIDES Administratoren an den Instituten mit der Berechtigung ausgestattet, Rechte an Personen weiterzugeben. Die Definition von Rollen erfolgt ausschließlich zentral durch die SIDES Systemadministration. Jede Rolle erhält einen Namen und eine kurze Beschreibung.

Nun sind Sie also mit einer Rolle und mit Rechten ausgestattet. Und möchten wahrscheinlich sofort ausprobieren, was sich damit machen läßt.

Es stehen FoDok-Online, Publikationseditor, Rechte-Manager und LVA-Editor zur Auswahl. All diese Anwendungen werden durch das SIDES Autorisierungssystem geschützt.

Nehmen wir an, Sie sind Mitarbeiterin bzw. Mitarbeiter im Sekretariat eines Institutes und würden gerne die Lehrveranstaltungen des Institutes editieren. Sie entscheiden sich also für den LVA-Editor und rufen diesen über `http://www.lzk.ac.at/sides/lva/tuwien/editor.htm` auf. Und: Fehlermeldung „Authorisation failed“. Über die Seite mit der URL `http://www.lzk.ac.at/sides/rechte` können Sie Ihre Rechte abrufen. Und siehe da: es sind noch keine Rechte für Sie vergeben. In diesem Falle wenden Sie sich bitte an den SIDES Administrator Ihres Institutes. Er oder sie kann unter Verwendung des Werkzeuges SIDES-Rechte-Manager (URL `http://www.lzk.ac.at/sides/rechte-manager`) Rechte an Personen weitergeben.

Sind Sie dann mit der Berechtigung „PRIV:LVA-Daten Exxx editieren“ (wobei „Exxx“ für die Kennzahl Ihres Institutes steht) ausgestattet, steht dem Bearbeiten der Lehrveranstaltungsbeschreibungen nichts mehr im Wege. Sicherheitssysteme sind stets mit der Problematik behaftet, einerseits möglichst einfach allen berechtigten Personen Zugang zu verschaffen, andererseits die Resourcen wirksam zu schützen. Das SIDES Sicherheitssystem kann zum Schutz statischer und dynamischer HTML-Seiten sowie von Java Applets verwendet werden.

Für die Benutzerin, den Benutzer ist lediglich eine einmalige Authorisierung erforderlich. Da diese unter Verwendung des White Pages Paßwortes erfolgt, ist auch hier kein zusätzlicher Aufwand erforderlich. Die Rechteadministration kann (weitgehend) dezentral erfolgen. Es steht mit der SIDES Authorisierungsinfrastruktur ein offenes und modulares System zur Verfügung, das für unterschiedlichste Anwendungen im Intranet-Bereich genutzt werden kann.

Ach ja, und viel Vergnügen mit Bachs Goldbergvariationen ...

Adressen:

- SIDES Hotline +43-1-58801-4136
- SIDES Systemadministration:
  Enzi Günter, LZK, +43-1-58801-4136
- SIDES Administratoren an den Instituten:
  `http://www.lzk.ac.at/sides/admin/`
- SIDES Homepage: `http://www.lzk.ac.at/sides`
- SIDES Status-Seite:
  `http://www.lzk.ac.at/sides/status`
- SIDES Rechteabfrage:
  `http://www.lzk.ac.at/sides/rechte`
- SIDES Rechte Manager:
  `http://www.lzk.ac.at/sides/rechte-manager`
- White Pages Address Manager:
  Martin Rathmayer, EDV-Zentrum, +43-1-58801-5834
- White Pages Dokumentation:
  `http://nic.tuwien.ac.at/nic/tuhb/white.htm`

Literatur:

SIDES Sicheres Internetbasiertes DatenErfassungsSystem für Publikations-und Lehrveranstaltungsbeschreibungsdaten an der TU Wien, Pipeline 21, Februar 1997, `http://info.tuwien.ac.at/pipeline/p21/sides.htm`

SIDES Lehrinformationssystem an der TU Wien, Pipeline 23, Oktober 1997, `http://info.tuwien.ac.at/pipeline/p23/sides.html`

Thomas Pauls, Günter Enzi
Österreichischer Lehrzielkatalog

SIDES ist ein Produkt des Österreichischen Lehrzielkataloges und wurde von Günter Enzi, Johannes Mayr, Martin Eller und Sebastian Fischmeister entwickelt.

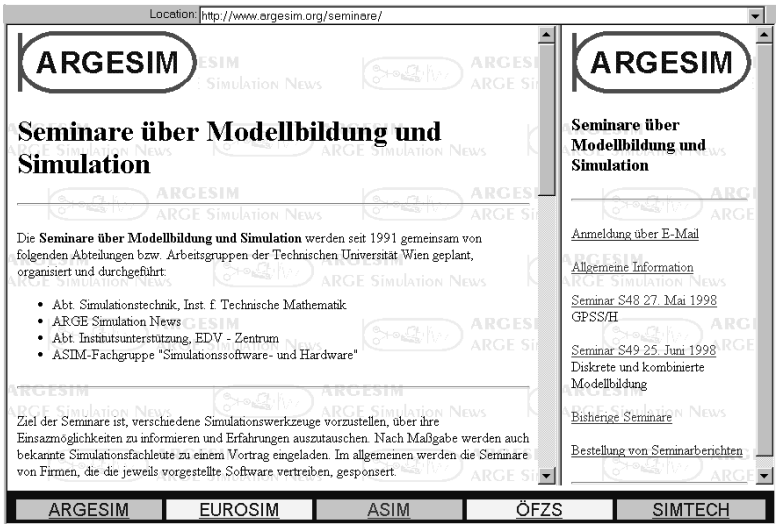
Seminare „Modellbildung und Simulation“

Zusammenarbeit Institutsunterstützung (EDV-Zentrum) und Abt. Simulationstechnik (E114)

ALLGEMEINES

Die Seminarreihe ***Seminare über Modellbildung und Simulation*** ist eine Gemeinschaftsveranstaltung der Abt. Simulationstechnik (Inst. f. Technische Mathematik, TU Wien), der Institutsunterstützung des EDV-Zentrums und der ARGESIM (Arbeitsgemeinschaft Simulation News, TU Wien). Bei größeren Seminaren fungiert auch die Fachgruppe „Simulationssoftware- und Hardware“ der deutschsprachigen Simulationsvereinigung ASIM als Mitveranstalter.

Im allgemeinen werden die Seminare von Firmen (den entsprechenden Software-Vertreibern) mitgesponsert oder über Simulationsprojekte der ARGESIM mitfinanziert. Dieses Sponsoring erlaubt auch immer ein kleines Buffet, das die Kommunikation zwischen Teilnehmern, Vortragenden, Firmenvertretern etc. fördert.



Informationen zu den Seminaren am ARGESIM-WWW-Server

Die Seminare dauern einen halben oder einen Tag. Die Teilnahme an den Seminaren steht allen an Modellbildung, Simulation und Engineering Tools Interessierten offen. Die Teilnehmer, von 30 bis 140 je Seminar (bisher 47 Seminare seit 1991), kommen zum Großteil von der TU Wien und von anderen Universitäten, aber auch aus Industrie, Dienstleistung und Verwaltung. Bei den bisherigen Seminaren waren etwa 20% der Teilnehmer aus der Industrie.

Die Teilnehmer werden um eine Anmeldung gebeten, daher können die Unterlagen, die zu Beginn des Seminars verteilt werden, schon eine Teilnehmerliste enthalten. Alle, die bereits an einem Seminar teilgenommen haben, werden automatisch zu den weiteren Seminaren eingeladen.

Weitere Informationen zu den Seminaren finden Sie am ARGESIM-WWW-Server, auch eine Anmeldung ist dort möglich:

`http://www.argesim.org/seminare`

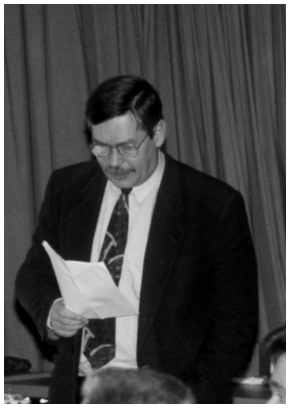
Wir gehen dazu über, weniger Einladungen per Post zu versenden, und mehr über Email zu arbeiten. Wir arbeiten an einem vernünftigen Konzept – und bitten im vorhinein um Entschuldigung, wenn Sie Email-Ankündigungen mehrfach erhalten. Vermutlich werden wir den Weg der HTML-Formate gehen.

Zum Veranstaltungsort: Bisher fanden die Seminare meist im Freihaus in Seminarräumen (oft im Physik-Seminarraum) statt, und nur bei großen Seminaren sind wir in den Kontaktraum in der Gußhausstraße ausgewichen. Seit diesem Jahr bemühen wir uns regelmäßig um den Kontaktraum, da die dortige Atmosphäre, insbesondere die relative Abgeschiedenheit, für Seminare geeigneter erscheint.

SEMINARE IM FRÜHJAHR 1998

In diesem Frühjahr fanden drei Seminare statt. Das erste Frühjahrsseminar war das alljährliche MATLAB-Seminar **„MATLAB und SIMULINK – Entwicklungen und Anwendungen“** am 12. 3. 1998, das bei weitem meistbesuchte Seminar.

Für die Veranstalter konnten Prof. Dr. F. Breitenecker (ARGESIM/SIMTECH), Dr. W. Kleinert (EDV-Zentrum) und Dr. H. Stahl (Fa. Scientific) etwa 140 Teilnehmer begrüßen – was im Veranstaltungsraum, dem Kontaktraum im Gebäude Gußhausstraße der TU Wien zu einigen Platzproblemen führte.



H. Stahl, F. Breitenecker und W. Kleinert begrüßen die Teilnehmer beim MATLAB-Seminar

In der Vorstellung neuer Produkte konzentrierte sich H. Stahl, der Geschäftsführer der Münchner Niederlassung des deutschen MATLAB-Distributors Scientific GmbH, einerseits auf die Stabilisierung und Konsolidierung der neuen MATLAB Version MATLAB 5 (Compiler, Datenbankinterface, Programmierung, neue Tool-

box-Versionen) und andererseits auf das Power System Blockset, mit dem der Simulator SIMULINK eine neue Ära beginnt: automatisierte graphische Modellerstellung auf Basis von nicht-kausalen graphischen Beschreibungsmethoden – im gegenständlichen Fall Leistungsgraphen-ähnlich.

Weitere derartige Blocksets für andere Anwendungsbereiche (z. B. Mechanik) sind bereits in Entwicklung; in der Diskussion stellte sich heraus, daß mit dieser neuen Beschreibungsform z.B. auch Bondgraphen direkt implementiert werden können.

Der Kontaktraum war bis auf den letzten Platz besetzt.

F. Breitenecker ergänzte diese Ausführungen mit einer kurzen Darstellung der Entwicklung der Lizenzierung an der TU Wien:

- Die idente Lizenzierung auf PCs und Workstations muß aufgegeben werden, u.a. da Third-Party Toolboxen nur unter PC angeboten werden und da Mathworks Originalversionen nur mehr für HP, SUN und SGI Workstations entwickelt (IBM und DEC Versionen werden nur bedingt „nachübersetzt“).
- Es wird weiterhin versucht, auf PC-Ebene eine „Volle Lizenzierung“ zur Verfügung zu stellen, auch unter Einbeziehung der Third-Party Toolboxen und Blocksets.
  So wurden auf Anregung von Benutzern die Delzer-Toolboxen IDCON und IDCON Nonlinear zur Identifikation, das MPA-Blockset und das Conti-Tool zur Vorbereitung von Mikroprozessor-Code sowie das Automatic Controller Design (ACD) Blockset angeschafft. Lizenziert wurden auch die Financial Toolbox sowie als wesentliche Neuerung in SIMULINK das Power System Blockset, und die Third-Party FCD Toolbox (Fuzzy Control Design).
- Bis Mai 1998 ist mit MATLAB Version 5.2 auf allen Plattformen zu rechnen, auch für MAC.
  Für MAC (nur Grundlizenzen) wird von Seiten Mathworks allerdings die Weiterentwicklung mit Version MATLAB 5.3 eingestellt!
- Trotz der Urgenzen vieler Benutzer wird die Linux-Version leider als reine UNIX-Version behandelt, was den LINUX Freaks das Arbeiten erschwert.

G. Hametner: Simulation eines geschwindigkeitsgeregelten hydrostatischen Antriebssystems bei Lastumkehr

F. Breitenecker schloß seine Übersicht mit dem Appell um mehr „Beitragswahrheit“ bei der Lizenzierung. Es sei klar,

- daß (im PC-Bereich) das Prinzip der Concurrency gelte und man MATLAB *n* mal lizenziert und *m* mal nutzt (installiert), $n < m$,
- daß aber ein Überziehen dieses Freiraumes auf $n << m$ unfair ist,
- und daß nur durch hinreichend viel „zahlende Benutzer“ weiterhin die Möglichkeit zur sehr weitreichenden Lizenzierung gegeben ist.

Der Vormittag beschäftigte sich zunächst mit allgemeinen Themenstellungen: H.-G. Feichtinger von der Universität Wien berichtete über numerische harmonische Analyse mit MATLAB, und E. Neuwirth entzauberte das Mysterium Wählerstromanalyse und Wahlhochrechnung, indem er seine diesbezüglichen MATLAB-Module vorstellte.

Ein weiterer Vortragsblock konzentrierte sich auf biologische Anwendungen: Abwasserreinigung, Müllentsorgung, physiologische Modelle (Lungenfunktion, Nervensystem).

Einen Schwerpunkt des Nachmittags bildeten Anwendungen in der Nachrichtentechnik: Mitarbeiter des Inst. f. Nachrichtentechnik der TU Wien stellten in fünf Beiträgen das breite Einsatzspektrum von MATLAB vor.

Weitere Kurzvorträge unterstrichen die zunehmende Bedeutung von MATLAB als Programmierwerkzeug für Prototyping und das Testen von Algorithmen.

Im letzten Vortragsblock stellten ARGESIM-Mitarbeiter die Möglichkeiten von Stateflow, der dritten wesentlichen Neuerung in MATLAB/SIMULINK, vor, vom klassischen Einsatz zum bequemen Ersatz komplexer logischer Schaltungen, über die Organisation von hybriden bzw. gemischten Modellen bis zur diskreten Simulation und Simulation von Markov-Ketten.

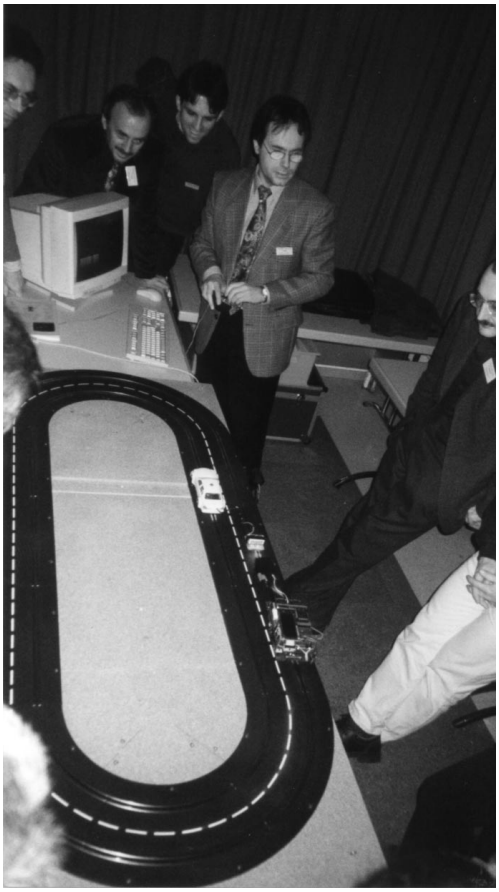
Der Vortrag von G. Hametner (Inst. f. Maschinendynamik und Meßtechnik) führte dann ein hochgradig nichtlineares Modell eines hydrostatischen Antriebes vor, mit Meßdatenvergleich und Identifizierung, und leitete damit zum letzten Vortrag mit Identifizierung und Echtzeitanwendung über.

Dieser letzte Vortrag von H. Stahl zeigte nochmals beeindruckend das breite Spektrum von MATLAB in Echtzeit- und HIL-Anwendungen auf und ließ auch die Herzen von Hobbybastlern höher schlagen: Auf einer Carrera-Autorennbahn wurde ein Fahrzeug händisch gesteuert, ein zweites folgte, automatisch gesteuert, in einem vordefinierten Abstand, wobei dieser Abstand mittels der Lichtintensität einer Leuchtdiode am ersten Fahrzeug gemessen wurde. Dabei wurden alle Aufgaben, vom Entwurf der Regelung bis zur Implementation auf dem Micro-Controller, mit Hilfe von MATLAB, Mathworks Toolboxen und Delzer Toolboxen gelöst.

Das Seminar endete um 19^{00} Uhr mit einer Verlosung von Preisen (als Dank für all jene, die bis zum Ende ausharrten – es waren etwa achtzig Personen): Abos von wissenschaftlichen Zeitschriften, Bücher zum Thema und MATLAB-Devotionalien.

In den Nachmittagspausen wurden bei einem „Basar" einige neue und viele leicht bis mittel veraltete MATLAB-Dokumentationen angeboten (aus unserem Fundus, bereichert durch eine Kiste mit alten Dokus von Scientific): der reißende Absatz erinnerte beinahe an Reinhard Mays Schlacht am kalten Buffet (das es übrigens – allerdings warm – auch zur Mittagszeit gab) und zeigt, daß Online-Dokus doch nicht der Weisheit letzter Schluß sind und das Ende von gedruckten User Guides noch lange nicht gekommen ist.

Im Rahmen des Seminars wurde auch über die Lizenzen und deren Weiterentwicklung an der TU diskutiert (siehe Beitrag „MATLAB QUO VADIS?" Seite 33, bzw. „Betreuung CAS" und „Betreuung MATLAB – ACSL", Seite 32) sowie über die Gestaltung des nächsten Seminars.



H. Stahl demonstriert die MATLAB-geregelte Verfolgungsfahrt

Dabei herrschte der Wunsch vor, das eintägige Seminar mit eher technischem Inhalt in der gegenwärtigen Form zu belassen und die vollkommen neuen Aspekte wie diskrete Modelle in Stateflow und Finanzmathematik in separaten Seminaren zu behandeln. Dem wird bereits durch das Seminar „Diskrete und kombinierte Modellbildung" (25. Juni 1998) teilweise Rechnung getragen.

Für die Gestaltung eines „kleinen" MATLAB-Seminars zum Thema Finanzmathematik, Ökonomie etc. werden Vorschläge, Vortragende und Interessenten gesucht. In diesem Zusammenhang sei darauf verwiesen, daß auch in der Österreichischen Nationalbank in einer Arbeitsgruppe MATLAB eingesetzt wird, und dringend nach MATLAB-Usern in ähnlichen Bereichen gesucht wird.

Im Vergleich zum MATLAB-Seminar im Vorjahr war wesentlich weniger Kritik zu hören. MATLAB scheint einerseits stabiler zu werden und die Bedürfnisse des Großteils der Anwender zufriedenstellen zu können, andererseits liegt eine gewisse Zurückhaltung auch in der Fast-Monopolstellung von MATLAB und der Tatsache, daß MATLAB eben „einfach da ist, wie es ist", vergleichbar dem Windows95.

Es ist zu hoffen, daß Mathworks mit der Monopolstellung vorsichtig umgeht.

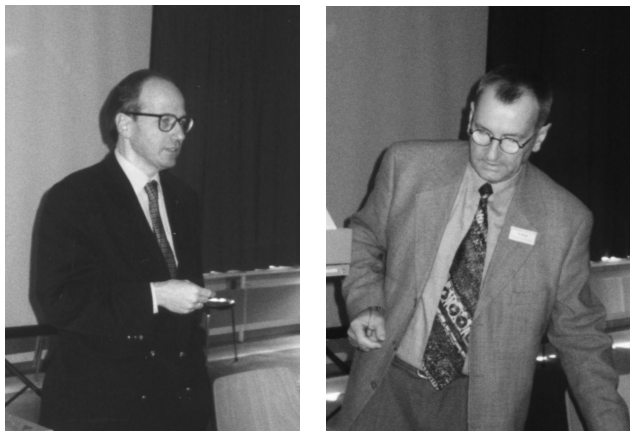
Knapp nach den Osterferien, am 21. 4. 98, fand das Seminar **„Computer Algebra Systeme (CAS)"** statt, das überraschend viele Interessenten anlockte.

Dieses Seminar beschäftigte sich auch allgemein mit CASen, und so konnte DI A. Blauensteiner (EDV-Zentrum) 63 Teilnehmer begrüßen und in Grundzügen die neue Zusammenarbeit des EDV-Zentrums mit der ARGESIM bei der Betreuung der Computer Algebra Systeme (ähnlich wie bei MATLAB) vorstellen.

Das Seminar bestand aus drei Teilen. Der erste Teil beleuchtete den Einsatz von CASen in der AHS/BHS- bzw. Undergraduate-Ausbildung. Dabei kam es zu einer höchst interessanten Diskussion zwischen H. Heugl, Landesschulinspektor für Mathematik in NÖ, der den Einsatz stark befürwortete und über Ergebnisse berichtete, und R. Taschner (TU Wien), der u.a. in der AHS-Lehrerausbildung tätig ist, und der ein höchst warnendes Bild zeichnete. Die Gegenüberstellung dieser sehr unterschiedlichen Ansichten erreichte das Ausmaß einer Grundsatzdiskussion, die nicht unwesentlich zu einer Verlängerung des Seminars führte.

Den Undergraduate-Teil schlossen die Vorstellung von „Maths and Fun" (ein Mathematica Notebook) durch R. Simonovits (HAK Graz) und Erfahrungsberichte mit „Maths and Fun" von P. Mazohl (Bundesgymnasium Babenbergerring, Wiener Neustadt) ab.

Der zweite Teil des Seminars stellte die an der TU Wien lizenzierten Produkte Mathematica, Maple und Derive in einer vergleichenden Studie gegenüber (F. Breitenecker), und die Fachbetreuer W. Auzinger und G. Betz berichteten über Neuerungen in Maple bzw. Mathematica.



R. Taschner und H. Heugl legen ihre Meinungen zum Thema CAS dar.

Aufschlußreich war der Vortrag „Haben CAS immer recht?" (H. Hlavacs, C.W. Überhuber), der kritisch Grenzen und Fehler der CASe betrachtete. Einen anwendungsorientierten Vergleich bot B. Gschaider beim Einsatz im Lagrange-Formalismus zur Herleitung mechatronischer Modelle.

Auch die Lizenzsituation an der TU Wien wurde kurz diskutiert. Die neuste Mathematica-Version (Mathematica 3.01) ist schon länger verfügbar. Maple kam mit der Version Maple V.5 heraus – und ist leistungsmäßig (vor allem in der Numerik) damit wieder eine Nasenlänge vor Mathematica; diese neue Version wird ab Mai zur Verfügung stehen. F. Breitenecker appellierte wie beim MATLAB-Seminar um eine Verbesserung der Beitragswahrheit bei der Lizenzierung, im PC-Bereich und vor allem im LINUX-Bereich.

In der Diskussion meinten Advanced Users, daß bei oftmaligem Einsatz von CASen sowohl Mathematica als auch Maple sinnvoll seien, da sie unterschiedliche Schwerpunkte in der Effizienz setzen und daher von Anwendung zu Anwendung einmal Maple und einmal Mathematica besser abschneidet.

Der dritte Teil des Seminars beschäftigte sich mit Anwendungen in der Simulationstechnik, sich auf das System Dymola konzentrierend. Dymola leitet aus Gesetzen durch symbolische Manipulationen Modellbeschreibungen in Zustandsraumdarstellung ab, die dann entweder direkt in Dymola simuliert werden können, oder die als ACSL-, SIMULINK- oder SIMNON-Modelle weitergegeben werden können.

Vorgestellt wurden von E. Forsthuber Dymola selbst und eine Simulationsstudie des Scara-Roboters (EUROSIM/ARGESIM Comparison 11) und von Th. Stefan (Inst. f. Elektrische Regelungstechnik) die Dymola-Simulation einer aktiven Netzrückspeisung.

Eine Testversion von Dymola ist über uns beschränkt erhältlich.

In einer regen Diskussion zur Kaffeepause wurde u.a. angeregt, das Seminar zu verlängern (auf ganztags) oder zwei Seminare zu veranstalten, das eine mit didaktisch-allgemeinem Inhalt, das andere technisch und simulationstechnisch orientiert. Für Meinungen und Hinweise sind wir dankbar – eine Neuauflage des Seminars ist für das Frühjahr 1999 geplant.

Als drittes Seminar fand am 22. 4. 98 das Seminar **„Graphische Modellbildung und Simulation diskreter Prozesse mit MicroSaint“** statt. Dieses Seminar hat – wie auch das Seminar über GPSS/H – eher Servicecharakter für Lehrveranstaltungen. Es stellte den Simulator Micro Saint vor und zeigte einige Anwendungen. R. Rainer (Inst. f. Statistik) gab anfangs einen Einleitungsvortrag über die statistischen Grundlagen der diskreten Simulation, von der Entstehungsgeschichte der Statistik bis zu den neuesten Werkzeugen, die zur Verfügung stehen.

SEMINARE IM SOMMER

Am 27. Mai 1998 findet das Seminar **„Diskrete Modellbildung und Animation mit GPSS/H – POWERSIM“** statt. Dieses Seminar ist – wie schon das Micro-Saint-Seminar – eher eine Serviceeinrichtung.

Es werden GPSS/H selbst sowie einige Anwendungen vorgestellt werden. Weiters wird SLX vorgestellt, das einerseits als GPSS/H-Nachfolger angesehen werden kann, andererseits eine C-ähnliche Implementierungssprache für diskrete Simulatoren auf verschiedenen Ebenen ist.

Im zweiten (kürzeren) Teil dieses halbtägigen Seminars wird der Simulator POWERSIM vorgestellt. POWERSIM bietet graphische Modellbildung für dynamische Prozesse auf Basis der System Dynamics Notation an und richtet sich damit vornehmlich an (kontinuierliche) biologische Prozesse, an einfache Fertigungsprozesse (Industrial Dynamics!) etc.

Das letzte Seminar im Sommersemester, **„Diskrete und kombinierte Modellbildung mit Stateflow – Model Maker“** am 25. Juni 1998, beschäftigt sich mit hybrider bzw. gemischter Simulation in Zusammenhang mit Stateflow einerseits, und mit den allgemeinen Möglichkeiten von Stateflow, der Finite-State-Machine von MATLAB/SIMULINK, andererseits, und richtet sich damit auch an „Advanced MATLAB Users“.

Es werden hybride Simulation am Beispiel des EUROSIM Comparison 7 (Constrained Pendulum), Simulation von Markov-Ketten und Petrinetzen u.ä. diskutiert.

Am Ende des Seminars wird der Simulator Model Maker vorgestellt, der eine graphische Modellbeschreibung in System-Dynamics-ähnlicher, aber verallgemeinerter Notation erlaubt und auch auf den Prinzipien der Kompartment-Modellbildung beruht.

SEMINARE IM WINTERSEMESTER 1998/1999

Ende des Sommersemesters findet das 49. Seminar statt, daher wird das erste Seminar im Wintersemester die Nummer 50 sein. Für dieses Seminar ist etwas Besonderes geplant. Das **Jubiläumsseminar** wird einen Leistungsbericht geben, und eingeladene Vortragende werden zu Grundsatzthemen sprechen.

Mit dem 51. Seminar (im Dezember) wird die letzte Wiederbelebung von ACSL versucht. Das letzte ACSL-Seminar (12. 1. 98) war sehr schwach besucht (trotz Terminverlegung und neuerlicher Einladungen).

Diese Tatsache ist leider mit dem generellen Rückgang von ACSL als allgemeiner Simulator begründbar (viele Anwender wechseln zu MATLAB/SIMULINK bzw. zu spezifischer Software, etwa FE-Systeme, Mehrkörpersysteme etc.). Es ist daher fraglich, ob ACSL weiter im Rahmen der Campuslizenz unterstützt werden kann (Lizenz bis Mitte 1999 vorhanden).

Für Jänner 1999 sind zwei Seminare zur biologischen Modellbildung und Simulation geplant. Dabei wird es zum einen um Simulation in der Medizin (regelungsmathematische Modelle vor allem des Herzkreislaufsystems), zum anderen um die Simulation von Abwasser- und Kläranlagen gehen.

Beide Seminare werden in Zusammenarbeit mit dem Österreichischen Forschungszentrum Seibersdorf (ÖFZS) veranstaltet werden, mit dem es dankenswerterweise schon bei früheren Seminaren eine gute Kooperation gab.

M. Lingl
ARGESIM / Abt. Simulationstechnik, Techn Univ. Wien

User Groups

Linux Usergroup „LLL“

Treffen: meist erster Mittwoch im Monat 14:00 an der TU. Genauere Angaben jeweils über die Mailing-Liste.

Homepage der LLL-Usergroup
(hier kann man sich auch für die Mailingliste anmelden):

`http://lll.ins.at/`

Weitere Links:
`http://iuinfo.tuwien.ac.at/`
(Plattform Support und dann Linux auswählen)

`http://radawana.cg.tuwien.ac.at/mail-archives/lll/`
(Mailarchiv der LLL-Mailingliste)

Windows NT Usergroup

Treffen: meist letzter Mittwoch im Monat 15:00 an der TU. Genauere Angaben jeweils über die Mailing-Liste und News.

Mailingliste:

Anmelden: eine Mail an
`listserv@iuinfo.tuwien.ac.at`
schicken, der „Mailbody“ muß folgende Zeile enthalten:

`subscribe winnt vorname zuname`

danach kann man über die Mailadresse
`winnt@iuinfo.tuwien.ac.at`
Mails an die Liste schicken.

Newsgruppe: `at.tuwien.os.winnt`

Computer Algebra Systeme

siehe auch Seite32

WWW: `http://argesim.tuwien.ac.at/compalgs`

NovAdmin-Meetings

Monatliche Treffen der Administratoren
von **Novell**-Servern an der TU

Zweck dieser regelmäßigen Treffen ist ein regelmäßiger Erfahrungs- und Gedankenaustausch:

- Neueinsteiger?
- Welche Hardware?
- Wer sind meine Mitkämpfer (die Betreuer der „anderen“ Novell-Server)
- Konfigurationen? Möglichkeiten?
- Zusatzprodukte?
- Diskussion über allgemeine Themen betreffs „Networking“

Hinweis: Sollten Sie Wünsche zu speziellen Themen bzw. Anregungen haben: Kontaktmöglichkeiten siehe unten.

Die nächsten Termine sind nachfolgender Liste zu entnehmen:

Donnerstag, 18. Juni 1998, 14.00 c.t.: (kein fixes Thema) (1)/(2)
(dies ist eine Änderung gegenüber den Terminen in der letzten Pipeline !!!)
Donnerstag, 9. Juli 1998, 14.00 c.t.: (kein fixes Thema) (1)
Donnerstag, 6. August 1998, 14.00 c.t.: (kein fixes Thema) (1)
Donnerstag, 10. Sept. 1998, 14.00 c.t.: (kein fixes Thema) (1)
Donnerstag, 8. Oktober 1998, 14.00 c.t.: (kein fixes Thema) (1)

(1).....Seminarraum 1, Floragasse 7 / Erdgeschoß
(2).....Dachterrasse d. Inst. f. Flexible Automation,
Floragasse 7a/ 4. Stock

Sollten Sie an einem Treffen, Aussendungen via E-Mail oder weiteren Informationen interessiert sein, so rufen Sie mich einfach an (Andreas Astleitner, E358, Tel.: 504 14 31-15) oder senden Sie mir eine Mail (`ast@novell.tuwien.ac.at`).

OS/2 User Group

`http://stud1.tuwien.ac.at/~e9125065`

Simulation

siehe auch Seite 32

WWW: `http://argesim.tuwien.ac.at/argesim`

Sekretariat

Montag bis Freitag
8 Uhr bis 13 Uhr

- Ausgabe und Entgegennahme von Formularen für Benutzungsbewilligungen für Rechner des EDV-Zentrums,
- Vergabe von Benutzungsbewilligungen für Benutzerräume,
- allgemeine Beantwortung von Benutzeranfragen, Weiterleitung an fachkundige Mitarbeiter.

Telephonische Anfragen: 58801-5481

Störungsmeldung:

Zentrale Server
Operating **58801-5830**
operator@edvz.tuwien.ac.at

TUNET
Tel.: **587 56 23**
Mail: **trouble@noc.tuwien.ac.at**

Wählleitungen:

01 / 589 32	**Normaltarif**
07189 15893	**Online-Tarif**

Datenformate:
300 - 56000 Bit/s (K56flex)
MNP5/V.42bis
SLIP/PPP
ISDN **Synchronous PPP**

Personelle Veränderungen

Anfang Juni beendet Herr Manfred Schandl nach 25-jähriger Dienstzeit seine Mitarbeit am EDV-Zentrum der Technischen Universität Wien und tritt seinen verdienten Ruhestand an. Manfred Schandl war über alle Jahre ein ausgesprochen liebenswürdiger und zuvorkommender, allseits beliebter Mitarbeiter, den wir bestimmt vermissen werden. Wir wünschen Herrn Manfred Schandl auf seinem weiteren Lebensweg von Herzen alles Gute.

Auch Frau Karin Schnelzer verläßt leider die Institutsunterstützung. Sie war durch ihr nettes Wesen und ihre verlässliche Arbeitsweise allen Mitarbeitern und speziell mir selbst eine wichtige und unschätzbare Hilfe.

Frau Christina Beisteiner arbeitet seit Anfang Mai im adminstrativen Bereich, Herr Dipl.-Ing. Markus Klug im Bereich des Campussoftware Setups der Institutsunterstützung.

Albert Blauensteiner

Herr Dr. Willy Weisz hat Anfang Februar 1998 das EDV-Zentrum der TU Wien verlassen. Er wechselte zum European Center for Parallel Computing at Vienna (VCPC) an der Universität Wien. Wir wünschen ihm in seinem neuen Wirkungsbereich viel Erfolg.

An seiner Stelle betreut seit April Herr Dipl.-Ing. Ernst Haunschmid, bisher Vertragsassistent am Institut für Numerische Mathematik, den Applikationsserver Lineare Algebra und ist für Leistungsmessungen, Optimierung von Applikationen und Compilerfragen zuständig.

Mitarbeiter

Telefonliste
E-Mail-Adressen
WWW-Adressen

EDV-Zentrum der
Technischen Universität Wien
Wiedner Hauptstraße 8-10
A - 1040 Wien
Tel.: (01) 58801-5481
Fax: (01) 587 42 11

WWW: http://www.edvz.tuwien.ac.at/

Hinweis: *Ab 7. September 1998 gibt es auch für das EDV-Zentrum neue, fünfstellige Telefonklappen. Sie werden rechtzeitig in den News und im WWW bekanntgegeben werden.*

Vorstand
o.Prof. Dr. S. Selberherr (3855)

vorstand@edvz.tuwien.ac.at
selberherr@iue.tuwien.ac.at

Leitung
W. Kleinert (5480)

kleinert@edvz.tuwien.ac.at
leiter@edvz.tuwien.ac.at

Administration
(Sekretariat): 5481

administration@edvz.tuwien.ac.at
sekretariat@edvz.tuwien.ac.at

A. Müller	5485	mueller@edvz.tuwien.ac.at
M. Haas	5489	haas@edvz.tuwien.ac.at

Anwendung von Informationssystemen / Ausbildung
D. Schornböck (5820)

schornboeck@edvz.tuwien.ac.at

I. Husinsky	5484	husinsky@edvz.tuwien.ac.at
E. Widmann	5486	widmann@edvz.tuwien.ac.at

Institutsunterstützung
A. Blauensteiner (5493)

blauensteiner@edvz.tuwien.ac.at
IU-Service-Line (5831)
WWW: http://iuinfo.tuwien.ac.at/

C. Beisteiner	5488	beisteiner@edvz.tuwien.ac.at
E. Donnaberger	5814	donnaberger@edvz.tuwien.ac.at
G. Gollmann	5848	gollmann@edvz.tuwien.ac.at
G. Kircher	5599	kircher@edvz.tuwien.ac.at
A. Klauda	5496	klauda@edvz.tuwien.ac.at
M. Klug	5855	klug@edvz.tuwien.ac.at
U. Linauer	5874	linauer@edvz.tuwien.ac.at
H. Mayer	5603	mayer@edvz.tuwien.ac.at
J. Peez-Donatowicz	5843	peez-donatowicz@edvz.tuwien.ac.at
E. Schörg	5482	schoerg@edvz.tuwien.ac.at
R. Sedlaczek	5858	sedlaczek@edvz.tuwien.ac.at
W. Selos	5606	selos@edvz.tuwien.ac.at
B. Simon	5602	simon@edvz.tuwien.ac.at
A. Sprinzl	5841	sprinzl@edvz.tuwien.ac.at
W. Steinmann	5842	steinmann@edvz.tuwien.ac.at
P. Torzicky	5494	torzicky@edvz.tuwien.ac.at

Kommunikation
J. Demel (5829)

demel@edvz.tuwien.ac.at
WWW: http://nic.tuwien.ac.at/nic/

F. Blöser	5810	bloeser@edvz.tuwien.ac.at
E. Donnaberger	5814	donnaberger@edvz.tuwien.ac.at
J. Haider	5823	jhaider@edvz.tuwien.ac.at
P. Hasler	5608	hasler@edvz.tuwien.ac.at
H. Kainrath	5811	kainrath@edvz.tuwien.ac.at
J. Kondraschew	5483	kondraschew@edvz.tuwien.ac.at
F. Matasovic	5605	matasovic@edvz.tuwien.ac.at
M. Rathmayer	5834	rathmayer@edvz.tuwien.ac.at
M. Schenner	5828	schenner@edvz.tuwien.ac.at
M. Siegl	5604	siegl@edvz.tuwien.ac.at
Walter Weiss	5605	weiss@edvz.tuwien.ac.at

Zentrale Services
P. Berger (5815)

berger@edvz.tuwien.ac.at
WWW: http://www.edvz.tuwien.ac.at/zserv/

W. Altfahrt	5819	altfahrt@edvz.tuwien.ac.at
J. Beiglböck	5495	beiglboeck@edvz.tuwien.ac.at
P. Deinlein	5830	deinlein@edvz.tuwien.ac.at
H. Eigenberger	5830	eigenberger@edvz.tuwien.ac.at
H. Flamm	5601	flamm@edvz.tuwien.ac.at
H. Fichtinger	5825	fichtinger@edvz.tuwien.ac.at
W. Haider	5492	haider@edvz.tuwien.ac.at
E. Haunschmid	5818	haunschmid@edvz.tuwien.ac.at
M. Krausz	5821	krausz@edvz.tuwien.ac.at
W. Leithner	5833	leithner@edvz.tuwien.ac.at
H. Mastal	5816	mastal@edvz.tuwien.ac.at
F. Mayer	5505	fmayer@edvz.tuwien.ac.at
J. Pfennig	5830	pfennig@edvz.tuwien.ac.at
A. Roza	5824	roza@edvz.tuwien.ac.at
J. Sadovsky	5487	sadovsky@edvz.tuwien.ac.at
G. Schmitt	5600	schmitt@edvz.tuwien.ac.at
E. Srubar	5826	srubar@edvz.tuwien.ac.at
G. Vollmann	5825	vollmann@edvz.tuwien.ac.at
Werner Weiss	5830	weisswer@edvz.tuwien.ac.at