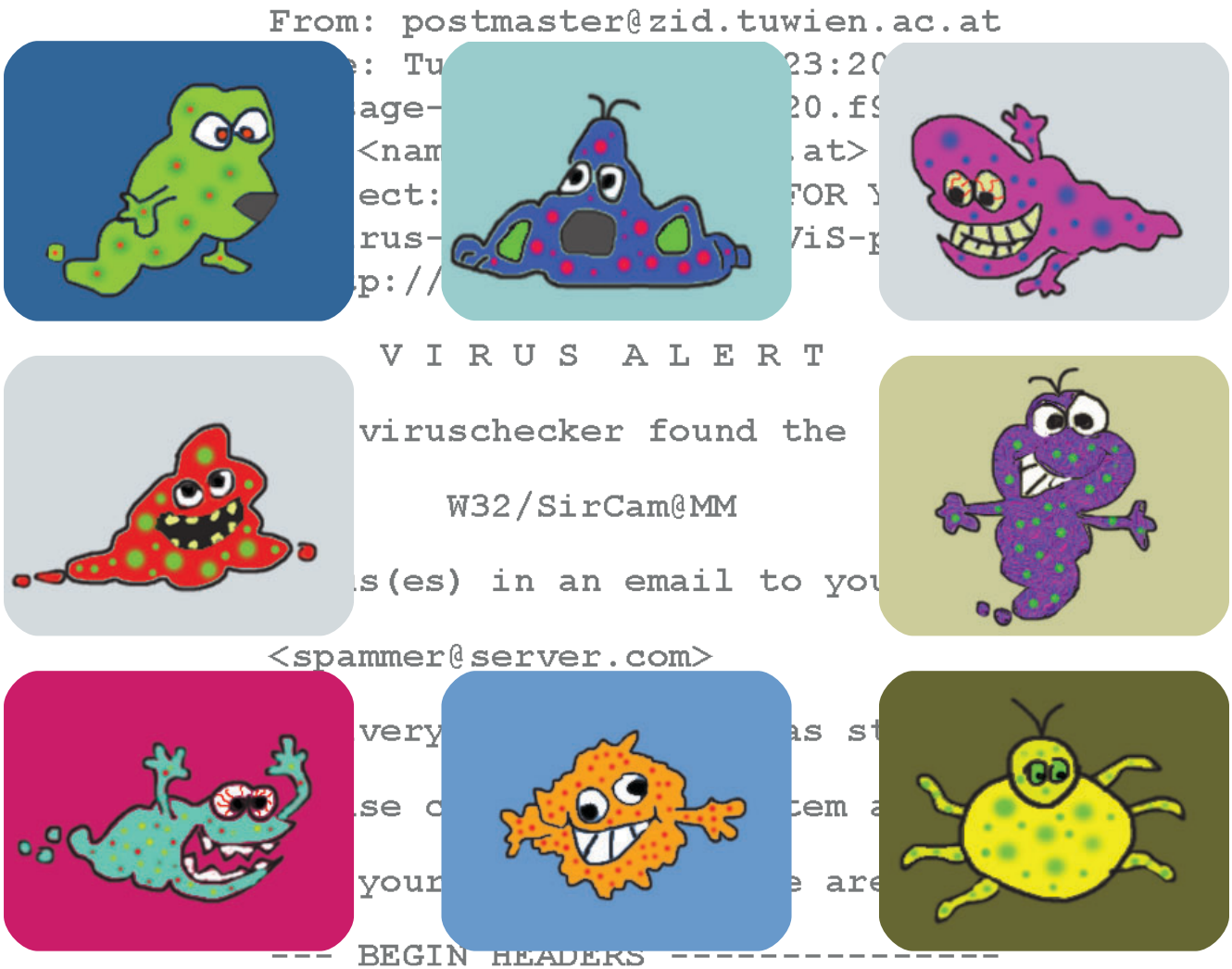
Nr. 6 / Dezember 2001

ISSN 1605-475X

ZID line

INFORMATIONEN DES ZENTRALEN INFORMATIKDIENSTES DER TU WIEN



Maßnahmen gegen Viren und Spam

Linux in den Internet-Räumen

Campussoftware Distribution

Inhalt

Impressum / Offenlegung gemäß § 25 Mediengesetz:

Herausgeber, Medieninhaber:
Zentraler Informatikdienst
der Technischen Universität Wien
ISSN 1605-475X

Grundlegende Richtung: Mitteilungen des Zentralen Informatikdienstes der Technischen Universität Wien

Redaktion: Irmgard Husinsky

Adresse: Technische Universität Wien,
Wiedner Hauptstraße 8-10, A-1040 Wien
Tel.: (01) 58801-42014, 42001
Fax: (01) 58801-42099
E-Mail: zidline@zid.tuwien.ac.at
WWW: http://www.zid.tuwien.ac.at/zidline/

Erstellt mit Corel Ventura
Druck: HTU Wirtschaftsbetriebe GmbH,
1040 Wien, Tel.: (01) 5863316

Editorial

Ein Hauptthema dieser ZIDline ist die zunehmende Viren- und Spam-Problematik bei E-Mails. Der ZID ist gefordert, Maßnahmen anzubieten, um die Situation für die Benutzer an der TU Wien zu verbessern.

Laufend können wir über Qualitätsverbesserungen der Internetanbindung der TU Wien berichten. Wir danken Herrn Dr. Rastl, dem Leiter des ZID der Universität Wien, für die Überlassung seines aktualisierten Beitrags über ACOnet 2001 aus dem *Comment* 01/3, der Schwester-Zeitschrift an der Uni Wien.

Für die Internet-Räume wurde ein neues Konzept erarbeitet, das auf Thin Clients unter Linux in Kombination mit Windows Terminal Servern basiert.

Die Serie über „Sicherheit unter Linux“ wird mit einem Artikel über Packet Filter fortgesetzt.

Das umfassende Angebot an Campussoftware erfordert leistungsfähige Server und eine effektive Software-Infrastruktur. Der neue Software Distribution Server wird vorgestellt und ein Überblick über die Online-Bestellung und Installation von Campussoftware gegeben.

Ein Anwenderartikel beschreibt die Erfahrungen am Institut für Allgemeine Physik mit dem Programm LabVIEW in der Experimentsteuerung.

Ich möchte mich an dieser Stelle herzlich bei allen Autoren dieser Ausgabe für ihre Beiträge und bei allen Mitarbeitern für die gute Zusammenarbeit bedanken.

Mit den besten Wünschen für 2002

Irmgard Husinsky

`www.zid.tuwien.ac.at/zidline/`

Viren am Titelblatt: I. Husinsky/A. Klauda

Frage: *„Kann durch eine Digitalkamera ein Virus in ein Computersystem gelangen ?“*

Antwort: *„Klar, wenn es Ihnen gelingt, eines zu fotografieren.“*

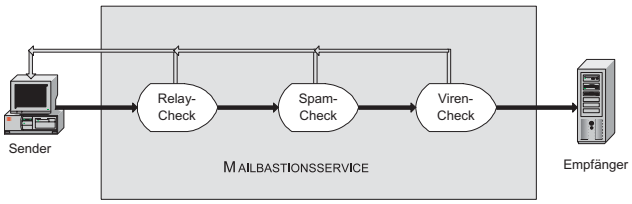
aus: PC Magazin, September 2001

Zentrale Anti-Viren-Maßnahmen

Udo Linauer, Johann Haider

Die Infektion mit aggressiven Computerviren über Mail führte immer wieder zu Ausfällen von Computern im TUNET, die nur mit erheblichem Arbeitsaufwand wieder zu beheben waren. Ein weiteres Problem stellen die zahllosen Spam-Mails dar. Der ZID erhält regelmäßig Beschwerden über Spam-Mails, die von der Mehrzahl der Mitarbeiter an der TU Wien als Belästigung empfunden werden (dazu mehr im Artikel „Zentrale Anti-Spam-Maßnahmen“, Seite 6).

Aufgrund wiederholter Anfragen seitens der Institute erweitert der ZID das Mailbastionsservice [1] um einen zentralen Virenscanner und einen Spam-Filter für eingehende Mail. Absolute Sicherheit können wir nicht garantieren, die Erfahrungen aus dem Testbetrieb versprechen jedoch eine drastische Verbesserung der momentanen Lage !



Zentraler Virencheck

Seit Jahren bedrohen Computerviren [2], Trojanische Pferde, Computerwürmer und dergleichen (zurzeit sind ca. 65000 bekannt) vorwiegend Rechner mit Microsoft-Betriebssystemen. Aus diesem Grund bietet der ZID im Rahmen der Campussoftware [3] Antiviren-Software zu extrem günstigen Konditionen an. Der Einsatz solcher Software am Arbeitsplatz ist eine höchst empfehlenswerte Selbstschutzmaßnahme für den sicheren Betrieb eines Computers (siehe auch Security Policy [4]) und kann durch keine zentrale Sicherheitsinfrastruktur komplett ersetzt werden !

Die Infektion mit Viren erfolgt über Diskette, CDROM oder beim Surfen im Web (aktive Inhalte oder Download), erfahrungsgemäß aber vor allem durch verseuchte Mail-Anhänge (Attachments). Die Einrichtung eines zentralen Virenscanners für Mails durch den ZID im Rahmen des Mailbastionsservices wird diese Gefahr in Zukunft vermindern. An dieser Stelle möchten wir in Erinnerung rufen, dass das Mailbastionsservice als Schutz für unsere Mailserver gegen Missbrauch durch Externe implementiert wurde. Es ist asymmetrisch und kann prinzipiell keinen Schutz vor internen Attacken bieten. Dieser Umstand gibt uns die Möglichkeit, automatisch, ohne Umkonfiguration (!) seitens der Benutzer, Virenschutz für alle Mails zu bieten, die von „außen“ an die TU Wien gelangen. Damit ist schon viel gewonnen, weil die meisten Viren zuallererst einmal von außen kommen und dann über die TU Wien weiter verbreitet werden. Automatischen Schutz auch für abgehende Mails genießen die Benutzer der vom ZID betriebenen Server (mail.zserv, pop, stud3, stud4, Applikationsserver).

Instituts-Mailserver

Schutz für abgehende Mail kann durch explizite Angabe des abgehenden Mailrouters (`mr.tuwien.ac.at`) zum Versenden von Mails erreicht werden. Für einen Mailserver geschieht dies durch Angabe eines „Smart Relay Hosts“ (siehe unten). Alternativ dazu können Benutzer ihren Mail-Client umkonfigurieren. Dafür muss im Mailprogramm `mr.tuwien.ac.at` als „Ausgehender Mailserver“ („Outgoing Mail Server“) eintragen werden. Weiters muss der Instituts-Firewall, falls vorhanden, den Zugriff auf `mr.tuwien.ac.at` gestatten. Wenden Sie sich bei Problemen an Ihren lokalen Systemadministrator oder die Computer Help Line des ZID, DW 42124 (bei aufrechtem Servicevertrag [5]). Dieses Service steht nur Benutzern im TUNET zur Verfügung.

Funktionsweise

Die Mail wird vom Mailserver (Mailbastionsrechner) auf einen Rechner umgeleitet, der ausschließlich zum Virenscannen eingesetzt wird. Insgesamt vier solcher Server garantieren ausreichende Ausfallssicherheit. Wird kein bekanntes Virus gefunden, erfolgt die Zustellung der Mail in der bisher bekannten Weise. Wird ein Virus entdeckt, erhalten sowohl der Absender als auch der Empfänger vom Mailbastionsservice eine Mail, die auf die verseuchte Nachricht hinweist. Diese Mail enthält Absender, Empfänger, Beschreibung des gefundenen Virus und die Mail-Header, so dass die beteiligten Benutzer feststellen können, wer die Nachricht gesendet hat. Die verseuchte Mail selbst wird nicht zugestellt. Bei ausgehenden oder internen Mails, also bei der Verwendung des abgehenden Mailrouters (`mr.tuwien.ac.at`), kommen dieselben Mechanismen zum Einsatz, mit dem kleinen Unterschied, dass der „externe“ Empfänger nicht von dem Zustellversuch informiert wird.

Informationen zu Anzahl und Art der abgefangenen Viren können auf der Webseite

http://nic.tuwien.ac.at/services/mail/virstats.html

abgefragt werden.

Warnung

Es gibt keinen absoluten Schutz vor Viren (aber einen messbaren) ! Nicht für jedes neue Virus gibt es gleich ein Gegengift. Es können nicht alle Datenformate überprüft werden (z. B. verschlüsselte Mails). Accounts bei externen Providern (Hotmail etc.) werden aufgrund der verwendeten Protokolle in der Regel nicht vom Mailbastionsservice geschützt. Wir empfehlen daher trotz des zentralen Virenchecks auch weiterhin die allgemeinen Verhaltensregeln zum Schutz vor Viren zu beachten [6].

Technische Details

Alle von außerhalb erreichbaren zentralen Mailserver der TU Wien (derzeit 4 Stück) werden mit einem Virenscanner ausgestattet. Zu diesem Zweck wird jedem dieser Server ein weiterer Rechner zugeordnet, der das Überprüfen auf Viren übernimmt.

Hard- und Software-Ausstattung für den Scanrechner:

Dual Athlon 1.2 GHz
1 GB RAM
2x18 GB Disk
Red Hat Linux 7.2
amavis-perl-11 [7]
McAfee Viruscan 4.14 [8]

Die Kommunikation zwischen beiden Rechnern erfolgt über das Milter (=Mail Filter) Protokoll [9]. Die Aufgabe von amavis ist es, die Mail so aufzubereiten, dass der Virenscanner in der Lage ist, ein mögliches Virus zu entdecken, d. h. die Datenkonversionen, die vor oder beim Versenden der Mail durchgeführt wurden (z. B. Packen der Datei oder Mail-Transfer-Encoding: base64), werden wieder rückgängig gemacht.

Unterstützte Dateiformate:

Mail Transfer Encoding:	quoted printable, base64
Mail Encoding:	uuencoded, xxencoded, binhex, TNEF
Datenkompression:	gzip, compress, bzip2
Dateiarchive:	tar, Zip, RAR, LHA, Arc, Zoo, Arj

Wenn kein Virus entdeckt wird, wird die Mail an den Empfänger weitergeleitet, andernfalls wird das Weiterleiten der Mail unterbunden. In diesem Fall erhalten der Absender und der Empfänger eine virenfreie Benachrichtigung.

Benachrichtigung an den Absender, z. B.:

```
From: postmaster@troja.com
Date: Tue, 23 Oct 2001 23:20:43 +0200 (MET DST)
Message-Id: <200110232120.f9NLKhtM009183@troja.com>
To: <odysseus@ithaka.com>
Subject: VIRUS IN YOUR MAIL
X-Virus-Scanned: by AMaViS-perl11-milter (http://amavis.org/)

                V I R U S  A L E R T

Our viruschecker found the

        APStrojan

virus(es) in your email to the following recipient(s):

-> <city@troja.com>

Please check your system for viruses, or ask your system administrator
to do so.

For your reference, here are the headers from your email:

------------ BEGIN HEADERS ------------

Received: (from odysseus@localhost)
by tauris.com (8.9.3/8.9.3) id XAA04339
for city@troja.com; Tue, 23 Oct 2001 23:20:39 +0200 (MET DST)
Date: Tue, 23 Oct 2001 23:20:39 +0200 (MET DST)
From: Odysseus <odysseus@ithaka.com>
Message-ID: <4338.1003872040@ithaka.com>
Mime-Version: 1.0
To: city@troja.com
Subject: Horse
Content-Type: multipart/mixed; boundary="-"

------------ END HEADERS ------------
```

Benachrichtigung an den Empfänger, z. B.:

```
From: postmaster@troja.com
Date: Tue, 23 Oct 2001 23:20:47 +0200 (MET DST)
Message-Id: <200110232120.f9NLKlOY009193@troja.com>
To: <city@troja.com>
Subject: VIRUS IN MAIL FOR YOU FROM <odysseus@ithaka.com>
X-Virus-Scanned: by AMaViS-perl11-milter (http://amavis.org/)

                V I R U S  A L E R T

Our viruschecker found the

        APStrojan

virus(es) in an email to you from:

<odysseus@ithaka.com>

Delivery of the email was stopped!

Please contact your system administrator for details.

For your reference, here are the headers from the email:

------------ BEGIN HEADERS ------------

...

------------ END HEADERS ------------
```

Erste Resultate

Seit Mitte Oktober ist ein Virenscanner nach dem beschriebenen Schema für den ZID in Betrieb. Obwohl der Empfängerkreis relativ klein ist, wurden täglich Mails abgefangen, die ein Virus enthielten.

Virus	Anzahl
W32/SirCam@MM	142
W32/Nimda	9
W32/Magistr	6
W32/Anset@MM	6
W32/Nimda@MM	5
W32/Hybris.gen@MM	2
ZIP-Crash	1
W95/Kuang.GR	1
W32/Magistr.a.dam1	1

Tabelle: Viren von 15. 10. bis 15. 11.

Beispiel für den „Smart Relay Host“

Nur für Systemadministratoren in der Domäne `tuwien.ac.at` !

Um ausgehende Mail über den abgehenden Mailrouter zu verschicken, setzt man in der Datei `sendmail.cf` den Parameter DS auf `mr.tuwien.ac.at` (die DS Zeile ist wahrscheinlich schon vorhanden, nur der Wert ist zu ergänzen). Die Zeile sieht dann wie folgt aus:

```
DS mr.tuwien.ac.at
```

Zur Aktivierung muss `sendmail` neu gestartet werden. Dieselbe Funktionalität gibt es auch bei anderen Mailservern (z. B. unter Novell). Details finden Sie in der Dokumentation Ihres Systems oder können bei den Kontaktpersonen des Plattformservices des ZID (siehe [5]) erfragt werden.

Referenzen

[1] ZIDline 4, Dezember 2000: http://www.zid.tuwien. ac.at/zidline/zl04/mailbast.html

[2] c’t 21/2001, S140ff, Jürgen Schmidt, Sicherheitsrisiko Microsoft, Verlag Heinz Heise

[3] Norton Antivirus, McAfee VirusScan, Sophos AntiVirus: http://sts.tuwien.ac.at/css/

[4] http://www.zid.tuwien.ac.at/security/policies/secpol.html

[5] http://sts.tuwien.ac.at/pss/
http://www.tu-berlin.de/www/software/avprev.shtml

[6] http://www.bsi.de/antivir1/texte/hinweise.htm

[7] http://www.amavis.org/

[8] http://www.mcafee.com/anti-virus/

[9] http://www.sendmail.com/partner/resources/development/milter_api

Server-Zertifikate des Zentralen Informatikdienstes

TU Testzertifizierungsstelle:
`http://www.zid.tuwien.ac.at/security/testca/`

Fingerprints der Test-CAs und der von ihnen ausgegebenen Serverzertifikate:

Zertifikat der Root-Test-CA (PCA)
gültig von Dec 30 1999 bis Dec 26 2014
`MD5 Fingerprint=`
`0D:D9:02:9C:24:61:85:9E:72:59:93:28:68:3D:B3:7C`

Zertifikat der Server-Test-CA (SCA)
gültig von Dec 30 1999 bis Dec 27 2009
`MD5 Fingerprint=`
`03:2F:CB:C6:B6:5B:FC:00:C0:56:41:DF:CD:E9:AF:98`

Zertifikat der User-Test-CA (UCA)
gültig von Dec 30 1999 bis Dec 27 2009
`MD5 Fingerprint=`
`3C:B3:AC:1F:83:D0:C9:1E:3E:11:31:53:A0:F3:C9:88`

Server-Zertifikat von stud3.tuwien.ac.at
gültig von: Nov 15 2001 bis Dec 5 2002
`MD5 Fingerprint=`
`FC:4E:CB:FC:53:E5:09:9B:08:E9:84:76:C1:17:CC:0B`

Server-Zertifikat von stud4.tuwien.ac.at
gültig von: Nov 15 2001 bis Dec 5 2002
`MD5 Fingerprint=`
`8C:16:D0:EF:EA:40:BA:EE:96:FA:D5:39:4A:36:1A:EB`

Server-Zertifikat von mail.zserv.tuwien.ac.at
gültig von: Nov 15 2001 bis Dec 5 2002
`MD5 Fingerprint=`
`B7:4C:50:58:9D:8E:D6:E3:68:AF:62:36:BB:22:8B:E8`

Server-Zertifikat von studman.ben.tuwien.ac.at
gültig von Jan 18 2001 bis Jan 18 2002
`MD5 Fingerprint=`
`9F:DD:07:6D:73:5E:9C:E6:51:62:4E:D7:53:4B:46:E6`

Server-Zertifikat von swd.tuwien.ac.at
gültig von May 10 2001 bis May 25 2002
`MD5 Fingerprint=`
`88:08:46:AB:A8:B9:78:AA:35:EE:6B:AA:6A:CC:B4:20`

Fingerprints von „TC TrustCenter Class 2 CA“:
Server-Zertifikat von
info.tuwien.ac.at (Informationsserver für die TU Wien)
gültig von Mar 27 2001 bis Mar 27 2002
`MD5 Fingerprint=`
`90:F4:99:B5:6B:DC:71:D8:81:EE:CB:24:0E:03:19:4C`

Fingerprints der „self signed“ Serverzertifikate:
Server-Zertifikat von
iu.zid.tuwien.ac.at (Campussoftware Verwaltung)
gültig von Mar 1 1999 bis Mar 1 2002
`MD5 Fingerprint=`
`A0:FF:97:E3:25:5D:07:B9:20:CC:84:D6:88:05:EB:0F`

Zentrale Anti-Spam-Maßnahmen

Johann E. Klasek

Schon lange sind TUNET-Benutzer ein beliebtes Ziel von Spam-Mails aus aller Welt. Mittlerweile nimmt das Ausmaß dieser Form von unverlangt zugestellten E-Mails mitunter unangenehme Dimensionen an. Sowohl für die Benutzer bzw. Empfänger solcher E-Mails als auch die Server-Betreiber. Zudem kommen noch Folgeerscheinungen von nicht unmittelbar die TU Wien betreffenden Spam-Mails, die sich auf andere Weise bemerkbar machen und sich im Wesentlichen in der erhöhten Belastung der Bastionsrechner widerspiegeln (was bisher aber noch keinen Grund zur Besorgnis darstellte).

Die sich aus diesen teils bedrohlichen Entwicklungen ergebenden vier Problemfelder münden derzeit in entsprechenden Strategien, die versuchen, dem E-Mail-Missbrauch (auch unter Berufung auf das Telekommunikationsgesetz, TKG §101, [1]) entgegenzuwirken:

1. Das TUNET als Quelle von Spams wird unterbunden: Durch Einsatz von Mailbastionsrechnern wird derzeit erfolgreich das dem Ruf der TU nicht besonders zuträgliche und administrationsintensive 3rd-Party Relaying verhindert.
2. Spam-Mails mit TU-fremdem Ursprung sind mit gefälschtem TU-Absender versehen, und gelangen als Retourmail an die TU: Diese können (als Option) für gewisse Zielbereiche nach gewissen Adressmustern am Mailbastionsrechner blockiert werden.
3. Empfänger im Bereich des TUNET werden von Spam-Mails heimgesucht. Mittels Zugriffseinschränkungen von Absender-E-Mailadressen und Serveradressen, basierend auf nicht im DNS auflösbare Adressen, auf konkrete Vorfälle die TU Wien betreffend oder auf dynamische im Internet angebotene Blackhole-Listen mit globalem Status, werden derartige Spam-Mails blockiert.
4. E-Mails werden nach Viren- bzw. Wurmbefall untersucht und gegebenenfalls unterdrückt (bei entsprechender Benachrichtigung des Empfängers). Mehr dazu im Artikel „Zentrale Anti-Viren-Maßnahmen“ auf Seite 3.

Spam Mail Relaying

Maßnahmen zum ersten Problemfeld sind bereits in den letzten zwei Jahren umgesetzt worden, sodass mittlerweile die gesamte TU flächendeckend über den Bastionsrechner geleitet wird. Der Zugriff von außerhalb des TUNET auf TCP Port 25 des SMTP-Protokolls ist (im Wesentlichen bis auf die Bastionsrechner) gesperrt. Die Bastionsrechner – wie bereits in [2] vorgestellt – leiten dann die ankommenden E-Mails TU-intern weiter. Interessierte Empfänger können diese zusätzliche Zwischenstation einer erhaltenen E-Mail auch daran erkennen, dass die detaillierte Ansicht des Mail-Headers eine Received-Line mit bzw. von `tuvok.kom.tuwien.ac.at` oder `neelix.kom.tuwien.ac.at` enthält.

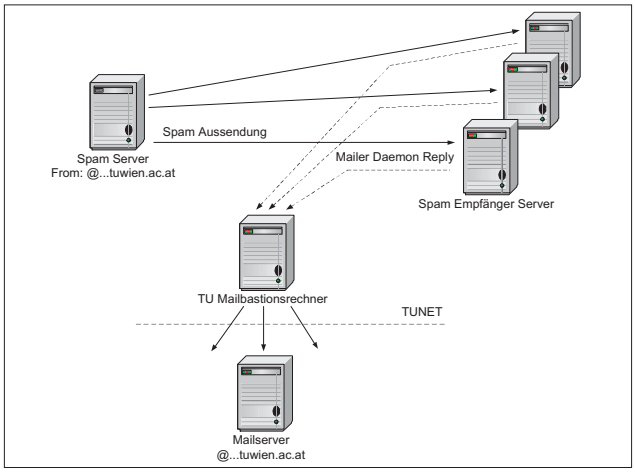
Beim Mailverkehr innerhalb des TUNET sind die Bastionsrechner nicht involviert, wobei z. B. die Wählleitungszugänge der TU Wien natürlich zum TUNET zu rechnen sind, nicht aber die TU Wien Chello Student Connect-Teilnehmer.

Einer speziellen Behandlung bedarf es bei so genannten „Externen Domains“ (also solchen, die nicht auf `tuwien.ac.at` enden), die auf TU Nameservern oder auch anderen, externen Nameservern betrieben werden und, was wesentlich ist, einen im TUNET befindlichen Mailserver verwenden wollen. Diese Domains bzw. deren Mailserver sind dann mit Begründung für den Zusammenhang mit den Aufgaben der TU Wien dem ZID zu melden (http://nic.tuwien.ac.at/formulare/domain.pdf), wodurch auch für diese externen Domains die Umleitung über die Bastionsrechner realisiert werden kann und somit dem Sicherheitskonzept genüge getan wird.

Spam Address Faking

Mit der zweiten Maßnahme tritt man einer Problematik entgegen, die mit Spam-Mails zum Vorschein kommen, die weder an der TU ihren Ursprung haben noch dorthin gesendet werden. Dennoch brechen schubweise und zeitlich gehäuft von unterschiedlichsten Mailservern des Internet wahre Mailstürme auf vermeintliche TU-

Mailadressen herein. Dabei handelt es um automatisch von Mailservern generierte Nachrichten, die offensichtlich von Spam-Mails herrühren, die an nicht (mehr) existierende oder anderweitig nicht erreichbare Empfänger gegangen sind und nun an den Absender zurück geschickt werden. Dabei agieren die Spam-Mail-Verteiler schon im Vorfeld so geschickt, dass sie als Absendeadresse ihrer Spam-Mails eine existierende Domain (eben eine der TU Wien) heranziehen und irgendwelche automatisch generierte User-Bezeichnungen (die vorab nicht überprüfbar sind) aus Ziffern und Buchstaben verwenden. Damit geht man als Spammer einer statischen Filterung auf die Absenderadresse und einer Blockierung von nicht-auflösbaren Adressen (bezieht sich immer nur auf den Domain-Teil einer E-Mail-Adresse) aus dem Weg. Explizit erwähnt soll hier die Tatsache sein, dass alle im Mail-Header gemachten Angaben, speziell die Adressen, beliebig gefälscht sein können und nicht für die Mail-Zustellung herangezogen werden (für eine Antwort-Mail allerdings dann schon). Die relevanten Zustelladressen werden direkt über das Simple Mail Transfer Protocol (SMTP) – entspricht dem Briefkuvert – gesondert übertragen und sind dann für Empfänger nicht mehr (direkt) sichtbar.



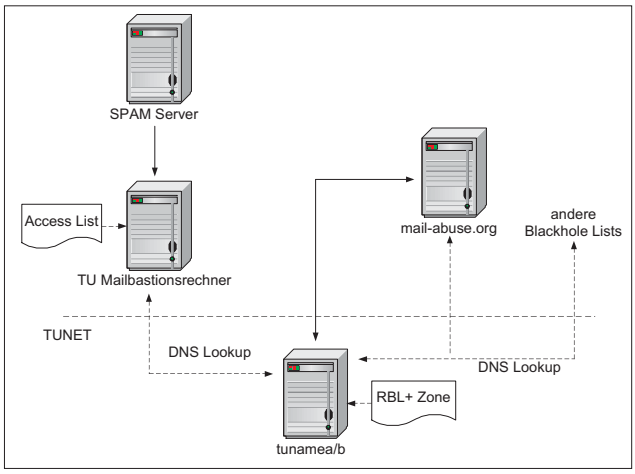
Konsequenzen von Sender Address Faking

Die Tatsache, dass so die TU Wien bzw. deren Bastionsrechner von den im Internet verteilten Mailservern mit derartigen Retourmails überschwemmt wird, kann durchaus als Distributed Denial of Service Attack (DDoS) gewertet werden, die zwar nicht auf diesen Effekt hin ausgerichtet ist, aber dennoch den ursprünglichen Spam-Mail-Versendern sehr wohl bewusst sein dürfte.

Da es sich in der Regel um Institutsdomains handelt, die auf diese Art missbraucht werden, sind natürlich auch die entsprechenden Instituts-Mailserver, an die diese Mails dann weitergeleitet werden, betroffen. Auch wenn am Institut die Fantasiebenutzer als Empfänger abgewiesen werden, kommt durch das Zwischenspeichern und das Verarbeiten jeder einzelnen Nachricht eine merkbare Belastung auf den Bastionsrechnern zustande. Aus diesem Grund bietet der ZID eine optionale Blockierung von speziellen Empfängeradressformen (User-Teil beginnt mit einem Buchstaben und endet auf mindestens zwei Ziffern), bezogen auf Hosts oder Subdomains der TU Wien Domain `tuwien.ac.at`, an. Bei Gefahr im Verzug wird die Errichtung der Blockade vorab durchgeführt und das Institut darüber informiert, um etwaige Konflikte mit der regulären Mailadressierung zu vermeiden. Auf Wunsch kann diese Blockade weiterhin permanent oder auch zeitlich begrenzt weitergeführt werden.

Spam Filtering

Die dritte Maßnahme bedient sich, in Anlehnung an die Empfehlung aus RFC 2505 (Anti-Spam Recommendations [3]), diverser Mechanismen, um direkte, an TU-Adressen gerichtete Spam-Mails abzuweisen.



Spam-Filter Arbeitsweise

Diese erzeugen bis heute zum Teil recht heftige Kontroversen bei Vertretern der Persönlichkeitsrechte, administrativen Organen von Firmen und Einrichtungen, kommerziellen Spam-Versendern und schließlich den eigentlichen E-Mail-Empfängern selbst. Im Falle der TU Wien werden optionale Methoden angeboten, die es erlauben, gewisse Verfahren abhängig von Empfängeradressbereichen auf Antrag zu aktivieren oder zu deaktivieren.

Konkret sind nun folgende Mechanismen implementiert bzw. vorgesehen:

1. **Nicht auflösbare Absender-Adressen** werden standardmäßig abgewiesen, d. h. wenn der Domainteil einer E-Mail-Adresse nicht mit einem Mailserver assoziiert werden kann oder kein Hostname ist (Überprüfung via DNS – Domain Name Service), wird die begonnene Verbindung abgebrochen und eine E-Mail-Übertragung kommt erst gar nicht zustande.
   Dabei können zwei unterschiedliche Situationen auftreten: Kann der Name z. B. wegen eines vorübergehenden Nameserverausfalls nicht überprüft werden, wird ein temporärer Fehler an den absendenden Mailserver retourniert, der es dann eine gewisse Zeit lang (in der Regel fünf Tage) weiter probiert. Hingegen wird bei einer negativen Antwort eines Nameservers die Abweisung durch einen permanenten Fehlerstatus angezeigt (was freilich so mancher Spam-Server ignoriert und dennoch weiter sendet) und an den Absender zurückgemeldet.
   Wenn ein derartiges Verhalten für ein Institut mit einer eigenen Mail-Domain nicht akzeptabel ist, besteht

die Möglichkeit, die entsprechende Subdomain von dieser Verfahrensweise auszunehmen.

2. **Manuelle Blockaden** aufgrund lokaler Vorfälle:
   Anzeichen wie die erhöhte Belastung der Bastionsrechner oder steigender Bandbreitenverbrauch bzw. abrupt angestiegene Mailtransferraten werden zum Anlass genommen, nach eingehender Prüfung manuelle Blockaden auf den Bastionsrechnern und den zentralen Mailservern zu errichten. Damit wird der Zugriff nach Kriterien wie
   - IP-Adresse des Absender-Mailservers oder
   - E-Mail-Adresse des Absenders (Benutzer oder die gesamte Domain)

   abgewiesen, wobei der Absender durch einen permanten Fehlerstatus auf das Nichtvorhandensein des gewünschten Empfängers hingewiesen wird (im Rahmen einer Retourmail durch das Mailsystem des Absenders). Wenn sich die Lage nach einiger Zeit stabilisiert hat, werden die Sperren wieder abgebaut.

3. **Blackhole Listen** (MAPS, ORDB, ORBZ, ...)
   Mit so genannten dynamischen Realtime Blackhole Lists (oftmals kurz als RBL bezeichnet), wie z. B. die diversen Listen der Mail Abuse Prevention System Organisation [4], ist eine globale, stets auf dem aktuellen Stand befindliche Datenbank über das normalerweise für die Namensauflösung im Internet zuständige DNS-System realisiert. Damit werden eingehende Mailverbindungen sofort überprüft, ob sie von gelisteten Mailservern, Dialup-Hosts und ungenutzten Adressbereichen stammen und gegebenenfalls blockiert. Es existieren einige derartige Systeme, die mit teils sehr unterschiedlichen bis hin zu verwirrenden Kriterien schwarze Schafe (Spammer-Systeme) sammeln, überprüfen und gegebenenfalls aus den entsprechenden Datenbanken wieder entfernen.

   Die TU Wien hat vorerst die Nutzung des erst kürzlich kostenpflichtig gewordenen RBL+ von Mail Abuse Prevention System (MAPS) beantragt und wird die Verwendung auf den TU-eigenen Nameservern zur Verfügung stellen. Die dafür notwendigen Nameservice Zonen liegen dort als Replikat vor, sodass entsprechende Anfragen nicht stets auf den externen MAPS-Nameserver zugreifen, was sonst je nach aktueller Erreichbarkeit zeitliche Verzögerungen mit sich bringen kann.

   Auf den Mailbastionsrechnern ist ein Service geplant, das wiederum auf Subdomain-Granularität das RBL-Verfahren auswählen lässt, ob und welche RBL-Varianten eingesetzt werden sollen. Mit MAPS als langjährigem Anbieter eines solchen Services (die RBL+ Liste umfasst etwa 470.000 Einträge) wird vorerst ein Anfang gesetzt, wobei durchaus auch andere RBL-Anbieter in Frage kommen können (z. B. ORDB mit etwa 120.000 Einträgen). Deren Verwendung sollte aber stets unter Bedachtnahme auf Konventionen, Bedingungen (wie man z. B. Server von einer Liste wieder weg bekommt) und technische Realisierung des jeweiligen Anbieters abgewogen werden. Dies wirkt sich in weiterer Folge auch auf die Angreifbarkeit solcher Services durch juristische Mittel aus. Kaum eines der länger im Umlauf befindlichen Services ist nicht in gerichtliche Auseinandersetzungen involviert gewesen, wovon man sich in den News-Kanälen der Web-Präsenz der Serviceanbieter überzeugen kann. Prominentestes Opfer in der jüngeren Vergangenheit war sicherlich die ORBS-Liste, die mit der Einstellung ihrer Tätigkeit just etliche Nachahmer (wie etwa ORDB [5] oder ORBZ [6]) gefunden hat.
   Zum Teil arbeiten Spam-Befürworter und sie unterstützende Provider derart eng zusammen, dass Nameserver der RBL-Betreiber aus gewissen Teilen des Internet schlecht oder gar nicht erreichbar sind. Im Internet verteilt agierende Nameserver hingegen unterstreichen hierbei die Stärke und das Durchsetzungsvermögen eines Services.

   In den Referenzen [4-9] finden sich einige Verweise auf Seiten diverser RBL-Serviceanbieter und Anti-Spam-Projekte, die hier kaum vollständig zitiert werden können, aber untereinander stark verwoben sind und damit zu allen Ecken der Anti-Spam-Gemeinschaft führen.

Viren

Das vierte und letzte hier genannte Problemfeld ist nicht unmittelbar mit der Spam-Problematik verbunden zu sehen, aber dennoch diesem gewissermaßen verwandt. Natürlich rufen via E-Mail verteilte Viren prinzipiell die gleichen unangenehmen Effekte (in den meisten Fällen noch schlimmere) hervor, die unerwünscht eingelangte Nachrichten zu Spam-Mails machen. Die zuvor erwähnten RBL-Anbieter tragen dieser Situation zum Teil Rechnung, in dem auch sonstige auffällige (etwa virenversendende) Mailserver bzw. allgemein formuliert, absendende Hosts aus dem Internet, in deren schwarze Liste aufnehmen, wobei dieser Ansatz meist mit der Verbreitungsgeschwindigkeit von Viren nicht mithalten bzw. deren Verbreitung effektiv verhindern kann. Ausführ-licheres zu diesem Thema ist im Artikel „Zentrale Anti-Viren-Maßnahmen“ auf Seite 3 nachzulesen.

Abschließend muss man dennoch feststellen, dass ganz gleich, welche Strategien auch immer zum Einsatz kommen, stets Lücken und Möglichkeiten für die Verbreitung von Spam-Mails und auch Viren auf E-Mail-Basis existieren werden. Die Dynamik des Internet und die teils starken kommerziellen Interessen hinter der Anwendung von Spam-Mails scheinen auch in Zukunft der Garant dafür zu sein.

Referenzen

[1] Telekommunikationsgesetz: http://www.tkc.at/WWW/RechtsDB.nsf/pages/TKG (TKG §101 Unerbetene Anrufe, Bgbl. I Nr. 188/1999 vom 20.8.1999)
[2] ZIDline 4, Dezember 2000, S. 3, Mailbastionsrechner - eine elegante Lösung der Spam-Problematik, http://www.zid.tuwien.ac.at/zidline/zl04/mailbast.html
[3] RFC 2505 Anti-Spam Recommendations for SMTP MTAs: ftp://ftp.isi.edu/in-notes/rfc2505.txt
[4] MAPS Realtime Blackhole List: www.mail-abuse.org,
[5] Open Relay Database: http://ordb.org/
[6] Open Relay Blackhole Zones: http://www.orbz.org/
[7] OsiruSofts Open Relay Spam Stopper: http://relays.osirusoft.com/
[8] Spam Prevention Early Warning System: http://spews.org/
[9] The Spamhaus Project: http://spamhaus.org/

Telekom-Projekt erfolgreich abgeschlossen

Wolfgang Kleinert

Am 31. 7. 2001 konnte nach erfolgreicher Schlussabnahme das Telekom-Projekt an der TU Wien endgültig abgeschlossen werden. Dies wurde durch eine gewaltige Schlussanstrengung von Management und Mitarbeitern der Auftragnehmer Telekom Austria und Ericsson Austria, des Planers und der Mitarbeiter des ZID erreicht. Dafür möchte ich allen Beteiligten herzlich danken.

In einem früheren Artikel (ZIDline 3, Juni 2000) hatte ich bereits die Komplexität und die Gründe für die aufgetretenen Verzögerungen bei unserem Telekom-Projekt ausführlich analysiert. Die dort beschriebenen Probleme konnten inzwischen alle zufrieden stellend gelöst werden. An der TU Wien ist jetzt ein Telekommunikationssystem realisiert, dessen technisches Konzept in einigen wesentlichen Punkten bis an die Grenzen des von der Telekommunikations-Branche Machbaren geht. Die Kombination von Desaster-toleranten Teilzentralen, die an einem ATM-Backbone gemeinsam mit der Datenkommunikation eines großen universitären Netzes betrieben werden, mit einem flächendeckenden DECT-System und einem chipkartenbasierten Verrechnungssystem, bei dem alle, durch extensive Verwendung von Least-Cost-Routing von mehreren Providern anfallenden Gebühren direkt an die Endbenutzer verrechnet werden (noch dazu mit der weiter gehenden Anforderung, dass mit einer Chipkarte sowohl Dienst- als auch Privat- und Projektgespräche durchgeführt und abgerechnet werden können), ist in dieser Form einmalig und zeigt, wozu die Telekommunikationsindustrie imstande ist.

Aus der Sicht unserer Endkunden war das Telekom-System bis auf immer wieder vereinzelt auftretende, unerklärliche Abbrüche von DECT-Gesprächen seit Sommer 2000 in den unspektakulären Dauerbetrieb übergegangen. Diese Probleme, die übrigens nicht nur an der TU Wien sondern weltweit aufgetreten sind, konnten nur durch eine Reihe von Software-Patches und einen Firmware-Upgrade in den DECT-Sendern und -Geräten einigermaßen zufriedenstellend gelöst werden, was einige Zeit in Anspruch nahm.

Als Betreiber musste der ZID allerdings darauf bestehen, dass alle Detailprobleme gelöst werden, die bei den Tests der für die Desaster-Toleranz wichtigen Group-Switch-Dopplung aufgetreten waren. Natürlich hoffen wir, dass ein Desaster-Fall wie Wassereinbruch oder Brand bei einer der Hauptanlagen im Freihaus oder am Karlsplatz nie eintreten wird, aber es mussten alle möglichen Fälle durchgespielt und das erwartete Systemverhalten demonstriert werden. Ebenso wichtig für den Betrieb des Gesamtsystems war die Beseitigung aller kleinen Fehler beim Datenabgleich des DNA-Servers mit den Daten der Zentralen Verwaltung und den White Pages sowie der Synchronisation mit der Telekommunikationsanlage MD 110.

Immer schneller: Gigabit-Netzwerke für die Wissenschaft

Peter Rastl
Zentraler Informatikdienst der Universität Wien
Peter.Rastl@univie.ac.at

Die Anbindung von Universitäten und Schulen an das weltweite Internet erfolgt im Allgemeinen nicht über den nächstbesten Internet-Provider, sondern wird in den meisten Staaten von eigenen nationalen Wissenschaftsnetzen (NREN – *National Research and Education Network*) erbracht. Auf diese Weise können die universitären Internet-Services landesweit gut koordiniert und wirtschaftliche Vorteile durch den gemeinsamen Einkauf größerer Netzkapazitäten und die Inanspruchnahme nationaler und internationaler Fördermittel genutzt werden. Außerdem sind gerade die Universitäten daran interessiert, neue technische Entwicklungen im Internet bereits einzusetzen, bevor sie am Markt allgemein verfügbar sind. Schließlich hat sich ja das Internet im universitären Bereich entwickelt und wurde hier jahrelang erfolgreich verwendet, ehe es seinen Siegeszug auch außerhalb der akademischen Welt antrat (siehe „Es begann an der Uni Wien: 10 Jahre Internet in Österreich", Comment 00/2, Seite 2 bzw. unter http://www.univie.ac.at/comment/00-2/002_2.html).

In Österreich wird das nationale Wissenschaftsnetz („ACOnet"), das allen gemeinnützigen Einrichtungen der Forschung, Bildung und Kultur zur Verfügung steht, nicht von einer selbständigen Organisation mit eigener Rechtspersönlichkeit, sondern vom Zentralen Informatikdienst der Universität Wien betrieben. ACOnet ist ein Backbone-Netz, das die Netzwerke der gegenwärtig 74 Mitgliedsorganisationen untereinander und mit dem Internet verbindet. Jede dieser Organisationen ist mit einer bestimmten Bandbreite, nach der sich auch der Kostenanteil für die Teilnahme an ACOnet richtet, an einen der acht ACOnet-Anschlusspunkte (PoP – *Point of Presence*) angebunden. Die ACOnet-PoPs befinden sich an der Uni Wien, der TU Graz, den Universitäten Linz, Salzburg, Innsbruck, Klagenfurt und Leoben sowie an der Fachhochschule Dornbirn.

Der ACOnet-Backbone – also die Verbindung dieser PoPs – wurde bisher mit ATM-Strecken der Telekom Austria betrieben, deren Bandbreite entsprechend den ständig steigenden Anforderungen typischerweise jedes Jahr verdoppelt wurde (zuletzt beispielsweise Wien–Graz 128 Mbit/s, Wien–Innsbruck 32 Mbit/s, Wien–Leoben 8 Mbit/s). Technisch gesehen sind heute allerdings auch im Weitverkehrsbereich bereits Bandbreiten von mehreren Gigabit pro Sekunde möglich. Damit werden im Internet neue Services realisierbar, die bisher nur im lokalen Bereich mit ausreichender Qualität genutzt werden konnten (z. B. Video-Streams).

Um an den Universitäten eine innovative Verwendung des Datennetzes zu stimulieren, etwa beim Einsatz der neuen Medien, sind Bandbreiten im Gigabit-Bereich erforderlich. Erst wenn das Netzwerk die Voraussetzungen für solche Anwendungen bietet, werden sie an den Universitäten Fuß fassen können. Deshalb hat der ZID der Universität Wien Ende vorigen Jahres die Umstellung des ACOnet-Backbone auf Gigabit-Bandbreiten in Angriff genommen: Sowohl die nationalen Backbone-Verbindungen als auch die internationale Internet-Anbindung werden derzeit massiv aufgestockt.

Im November 2001 wurden im Rahmen eines neuen Servicevertrags mit der Telekom Austria sechs der acht ACOnet-PoPs über Lichtwellenleiter mit einer Bandbreite von 1,25 Gbit/s verbunden (siehe Abb. 1); für die beiden Standorte Leoben und Dornbirn wird im nächsten Jahr eine Aufstockung auf 100 Mbit/s angestrebt. Diese neue, um eine Größenordnung leistungsfähigere Infrastruktur ermöglicht es, künftig den Datenverkehr innerhalb von ACOnet wie in einem LAN ohne Verkehrsbeschränkungen – abgesehen vom Gigabit-Limit – zu erlauben und nur die Bandbreiten für den Datenverkehr nach außen (ins nationale und internationale Internet) entsprechend

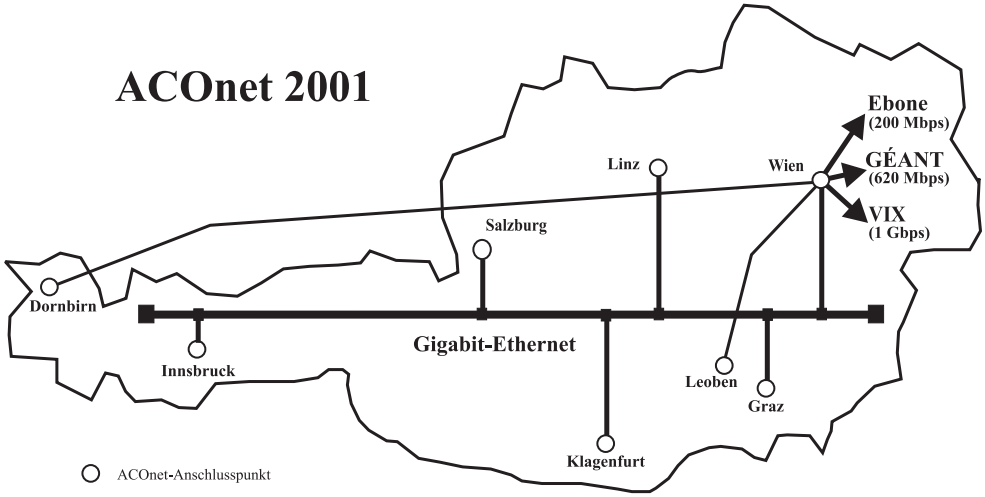


Abb. 1: Nationale und internationale ACOnet-Verbindungen ab November 2001

den von den ACOnet-Teilnehmern getragenen Kostenanteilen zu beschränken.

ACOnet betreibt seine externen Verbindungen über mehrere Anschlüsse: Die NRENs der meisten Staaten Europas und die an diese Wissenschaftsnetze angeschlossenen Institutionen sind über ein eigenes europäisches Wissenschaftsnetz untereinander verbunden, welches in Kooperation der europäischen NRENs mit finanzieller Unterstützung durch die EU-Kommission errichtet wurde. An dieses europäische Wissenschaftsnetz, das im Lauf der Jahre unter verschiedenen Namen (zuletzt: TEN-155 – *Trans European Network at 155 Mbps*) ständig ausgebaut wurde, war ACOnet zuletzt mit einer Bandbreite von 90 Mbit/s angeschlossen.

Die europäischen NRENs haben bereits 1999 ein Projekt unter dem Namen GÉANT gestartet, um ein Multi-Gigabit-Backbonenetz als Nachfolge für TEN-155 zu errichten. Dieses für 4 Jahre geplante Projekt mit einem geschätzten Kostenaufwand von 200 Millionen Euro wird von der EU-Kommission in ihrem 5. Rahmenprogramm

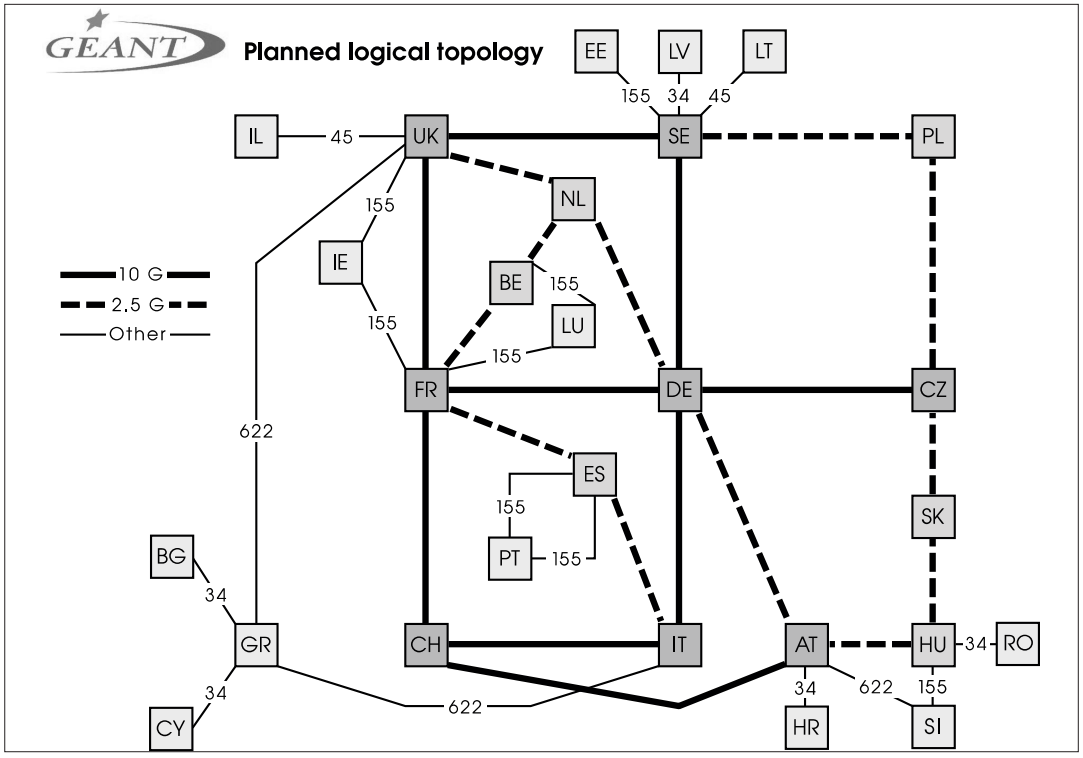


Abb. 2: Geplante internationale Verbindungen im europäischen Wissenschaftsnetz GÉANT

mit 80 Millionen Euro gefördert. Ein Konsortium von 27 NRENs (für 31 europäische Nationen) unter der Koordination von DANTE, einer für diesen Zweck von den NRENs gegründeten und in Cambridge (UK) beheimateten Non-Profit-Firma, ist für die Management-Entscheidungen im GÉANT-Projekt verantwortlich. Es ist geplant, auch leistungsfähige Verbindungen zu den Wissenschaftsnetzen in anderen Kontinenten zu errichten und innerhalb der vierjährigen Projektlaufzeit die Bandbreite im europäischen Backbone-Netz auf 100 Gbit/s zu erhöhen.

Im August 2000 hat DANTE eine europaweite Ausschreibung gestartet, um die für das GÉANT-Netz erforderlichen Datenverbindungen zu beschaffen. Nach einem aufwendigen Auswahlverfahren (immerhin waren Angebote von 31 Anbietern zu evaluieren) wurden schließlich am 5. Juli 2001 die Verträge mit den Bestbietern COLT Telecom, T-Systems (Deutsche Telekom) und Telia unterzeichnet, die den Kern des GÉANT-Netzes mit Bandbreiten von 10 bzw. 2,5 Gbit/s bereitstellen. Österreich ist dabei mit einer 10 Gbit/s-Verbindung nach Genf und einer 2,5 Gbit/s-Verbindung nach Frankfurt in dieses Netzwerk integriert und bildet auch den Anschlussknoten nach Ungarn, Slowenien und Kroatien (siehe Abb. 2). Das GÉANT-Netz ist im November 2001 in Betrieb gegangen; ACOnet wurde mit einer Bandbreite von 620 Mbit/s daran angeschlossen, was eine Steigerung um mehr als das Zehnfache gegenüber dem Vorjahr bedeutet.

Über den VIX (Vienna Internet eXchange; siehe Comment 01/1, Seite 30 bzw. http://www.univie.ac.at/comment/01-1/011_30.html) ist ACOnet mit den kommerziellen österreichischen Internet-Providern (und auch einigen ausländischen) verbunden. Die Verbindung zu sämtlichen Netzknoten im Internet, die nicht über den VIX oder über TEN-155 zu erreichen sind, stellt ACOnet durch einen Anschluss an Ebone, einen der führenden Internet-Backbones, her (derzeit 200 Mbit/s, ab 2002 620 Mbit/s). Dass alle diese Verbesserungen bei gleichbleibendem ACOnet-Budget (jährlich etwa 80 Millionen Schilling) möglich waren, gehört wohl auch zu den Erfolgen dieser Anstrengungen.

Weitere Qualitätsverbesserung bei der Internetanbindung der TU Wien

Johann Kainrath

Und es wächst und wächst und wächst ...
Laut einer aktuellen Studie der TeleGeography-Gruppe sind zwischen 2000 und 2001 die internationalen Internet-Bandbreiten um nicht weniger als 174 Prozent gewachsen, was mehr als einer Verdoppelung dieser entspricht. Von 1999 auf 2000 betrug die Steigerung der Bandbreite gar 382%. Für Europa ist damit die genutzte Bandbreite von 232 auf 675 GB/s gewachsen.

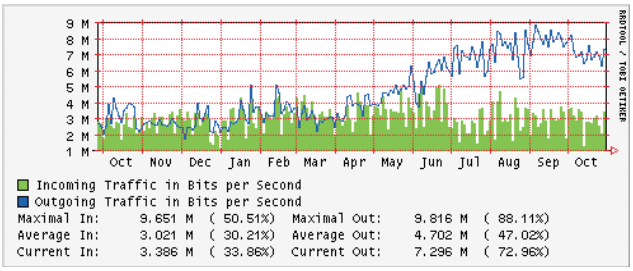
Neuer Provider COLT Telecom Austria GmbH

Das Bemühen, der TU Wien eine qualitativ hochwertige Internetanbindung zu garantieren, erfordert eine ständige Beobachtung der Internet-Serviceanbieter und deren Service-Qualität. Daher wurde im Herbst dieses Jahres die zweite Internetanbindung der TU Wien (Schwerpunkt internationaler Verkehr und USA) entsprechend rechtzeitig vor Ablauf des bisherigen Vertrags mit KPNQwest neu ausgeschrieben. Als Bestbieter wurde COLT Telecom Austria GmbH ermittelt.

Entwicklung seit dem Jahr 2000

Wie sicher bekannt, verfügt die TU Wien über zwei sehr leistungsfähige Anbindungen an das Internet. Anfang April 2000 wurde von AT&T Global Network Services (5 MBit/s) erstmals zu KPNQwest (6 MBit/s) gewechselt. Die ACOnet-Bandbreite betrug damals 16 MBit/s. Mit 2. November 2000 wurde die Internetanbindung über KPNQwest abermals erhöht, und zwar auf 8 MBit/s; am 2. Mai 2001 erfolgte die nächste Erweiterung auf 10 MBit/s. Die ACOnet-Verbindung hatte zu diesem Zeitpunkt bereits 32 MBit/s Kapazität. Die Bandbreitenentwicklung von Oktober 2000 bis Oktober 2001 (noch mit

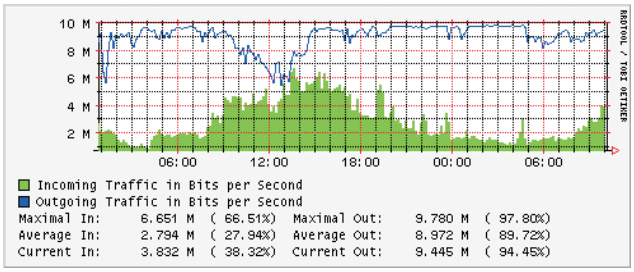
KPNQwest als Service-Provider) ist in nachfolgender Statistik dokumentiert.



Abgehender (dunkle Linie) und ankommender (graue Fläche) Verkehr der TU Wien im Zeitraum Oktober 2000 bis 2001 über die KPNQwest Verbindung.

Wie die Grafik deutlich zeigt, ist seit Juni die abgehende Belastung (also der Verkehr von der TU Wien in das Internet) extrem gestiegen. Mit ein Grund für diese Entwicklung war und ist die Verwendung von Applikationen auf dem Gebiet der Multimedia-Technologie. Dazu zählen die so genannten Peer-to-Peer Filesharing Tools.

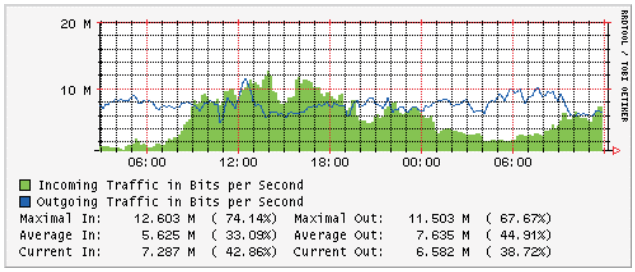
Hochlastsituationen (wie in der nachfolgenden Grafik zu sehen) auf der Internetverbindung treten zunehmend häufiger auf, dabei ist der abgehende Verkehr am „Anschlag“ und der eigentliche wissenschaftliche Nutzverkehr bleibt dadurch nicht mehr ohne Beeinträchtigung. Dieser Zustand wirkt sich natürlich auch auf den ankommenden Verkehr (Mail, Zugriff auf Web-Seiten im Internet, ...) aus.



Hochlastsituation abgehender Verkehr (dunkle Linie), ein Tag Anfang September 2001

Aktuelle Kapazität der Anbindung

Die Umstellung auf den neuen Provider COLT erfolgte am 31. 10. 2001 nachmittags. Die verwendete Technologie zur Anbindung basiert auf dem 100 MBit/s Ethernet Standard. Damit ist keine Abhängigkeit mehr von anderen Leitungsprovidern gegeben, denn COLT hat eine eigene Glasfaserstrecke bis in die TU Wien errichtet. Durch diese Realisierung ist weiters auch eine problemlose Kapazitätserweiterung ohne neuerlichen Installationsaufwand möglich.



Aktuelle Auslastung der COLT Verbindung (17 MBit/s) 12. bis 13. November 2001

Mit 1. November 2001 wurde diese zweite Internetanbindung der TU Wien nun mit insgesamt 17 MBit/s realisiert (wobei davon 4 MBit/s zu günstigeren Konditionen für das Goodie Domain Service reserviert sind).

COLT Telecom Austria GmbH ist ein Tochterunternehmen der COLT Telecom Group plc mit Sitz in London. Das Unternehmen ist auf Geschäftskunden ausgerichtet und betreibt in Wien ein eigenes hochleistungsfähiges Glasfasernetz zur Übertragung von Daten, Sprache und Multimedia-Applikationen.

ACOnet

Auch der Haupt-Provider der TU Wien baut seine Kapazitäten weiter aus und marschiert in Richtung Gigabit Ethernet. Siehe dazu den Artikel „Immer schneller: Gigabit-Netzwerke für die Wissenschaft“ von Peter Rastl, Leiter ZID der Universität Wien, in dieser Ausgabe der ZIDline.

Die Erhöhung der ACOnet-Bandbreite für die TU Wien auf 64 MBit/s wird noch im Quartal 4/2001 erfolgen.

Derzeit weist die Internetanbindung der TU Wien somit folgende Kapazität auf:

ACOnet	32 MBit/s
COLT	13 MBit/s
	+ 4 MBit/s für Goodie Domain Service

Einerseits ist dadurch der Bedarf an wissenschaftlicher Bandbreite auf sehr hohem Qualitätsniveau garantiert, andererseits werden zudem noch ausreichend Reserven für Projekte und sonstigen Datenverkehr geboten. Und dieser wird sicherlich durch den ständigen Ausbau der Wissenschaftsnetzwerke bzw. des Internet generell weiter kontinuierlich steigen.

Linux in den Internet-Räumen

Martin G. Rathmayer

**Die derzeitigen Benutzer-PCs in den Internet-Räumen des ZID laufen unter Windows 95 und werden übers Netzwerk gebootet. Das Konzept hat sich bis jetzt sehr gut bewährt, da es relativ gut administrierbar ist und eine sichere und stabile Arbeitsumgebung für den Benutzer bietet. Dieses System kann aus zwei Gründen nicht mehr länger aufrecht erhalten werden:
Zum Ersten ist die bestehende technische Lösung mit neuen Hardware-Komponenten nicht mehr realisierbar. Zum Zweiten ist ein Umstieg auf ein neueres Betriebssystem auf Grund moderner Applikationen dringend notwendig, allerdings wird das Prinzip des „Remote Network Boot" unter Windows ME, Windows 2000 oder zukünftigen Windows-Versionen nicht mehr unterstützt. Da eine lokale Installation bei einer so großen Anzahl von PCs nicht ausreichend wartbar ist, wurde ein anderer Weg, basierend auf Thin Clients unter Linux in Kombination mit Windows Terminal Servern, gewählt. Dieses neue Konzept ist sehr vielversprechend, da es flexibel und gut ausbaubar ist und die beiden zukünftigen großen Welten Linux und Windows miteinander verbindet.**

Konzept

Das neue System sieht wie bisher „diskless" PCs vor, die allerdings unter Linux laufen und darüber hinaus per geeigneter Client Software Zugriff auf eine spezielle Auswahl aktueller Windows-Applikation haben. Diese so genannten Thin Clients werden ebenfalls übers Netzwerk gebootet und greifen auch auf das „Home Directory" des jeweiligen Benutzers am UNIX Studentenserver zu. Das Konzept ist ähnlich der derzeitigen LBR/Mars Alternative und wird diese auch zur Gänze ablösen.

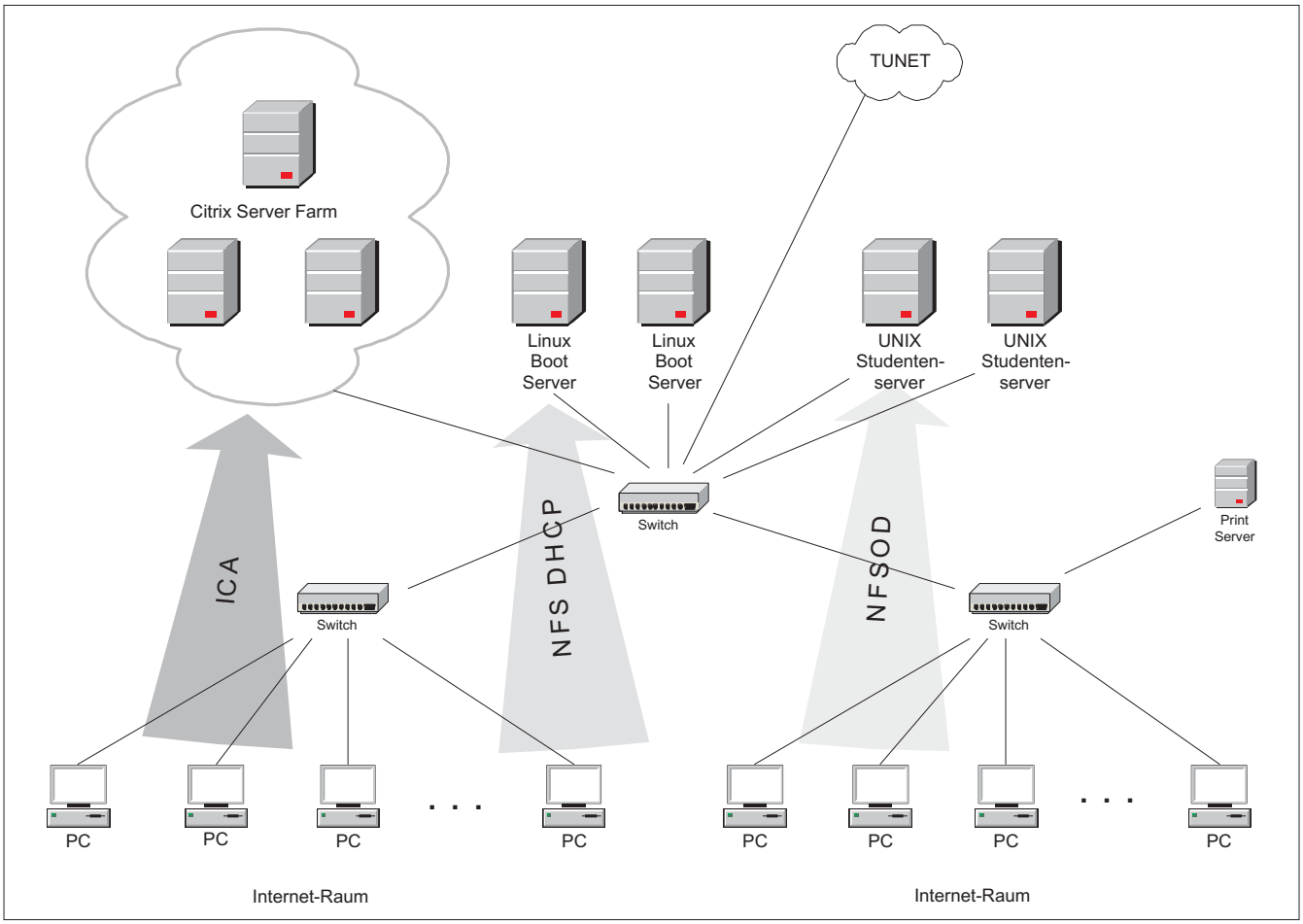
Die Bedienung einer Linux Workstation ist heutzutage bereits sehr komfortabel und nahezu „*Windows like*", sodass ein Umstieg auf dieses Betriebssystem ohne Probleme von einem Studenten der Technischen Universität Wien zu bewältigen ist. Auch steht bereits eine große Anzahl von guten Linux-Applikationen zur Verfügung, sodass der Standardbenutzer damit sicherlich sein Auslangen finden wird. Zusätzlich gibt es eine Citrix Windows Terminal Server Farm, auf der per ICA (*Independent Computing Architecture*) Client eine ausgewählte Anzahl von Standard Windows-Applikationen und eine Reihe spezieller Windows-Programme (z. B. für Übungen) ausgeführt werden können.

Thin Client Hardware

Die eingesetzten PCs haben alle 128-256 MB Hauptspeicher, Pentium II oder Celeron Prozessoren und teilweise CDROM-Laufwerke und Wheel-Mäuse. Einige Clients sind bereits mit 100 MBit/s ans TUNET angebunden und bieten sogar Audio-Unterstützung. Ein Parallel oder USB ZIP Drive kann überall angeschlossen werden. Alle Geräte besitzen deutsche Tastaturen und 17" Monitore. Alte, langsamere Geräte werden vollständig ersetzt. In Zukunft wird überall eine maximale Ausbaustufe angestrebt. Es ist ebenfalls geplant, die VT100 Terminals durch Kiosk PCs zu ersetzen.

Remote Boot Server Hardware

Die Linux Boot Server besitzen eine gute Netz- und I/O Performance für die NFS Verbindungen, d. h. schnelle SCSI-Platten und eine gute Bus-Bandbreite (Dual Pentium III mit mindestens 512 MB und zwei Netzwerkkarten). Ausfallssicherheit und Leistungssteigerung wird durch mehrere redundante Server (derzeit zwei Stück) erreicht, die von einem Master Server ihre Konfigurationen und von einem Reference Client ihre zu exportierenden Daten laden. Die Windows-Applikationen liegen auf



Linux Remote Boot in den Internet-Räumen

einer eigenen Server Farm (derzeit drei Rechner), die unter Windows 2000 mit Citrix Metaframe XP betrieben wird (siehe „Citrix Terminal Server für die Internet-Räume“, Seite 17).

Software

Als Basis dient die komplette Linux RedHat Distribution Version 7.x (Kernel 2.4.x) mit KDE (Version 2.x) als Desktop-Empfehlung. Im Wesentlichen werden die wichtigsten KDE-Applikationen für Mail/News/WWW vom ZID unterstützt sowie einige ausgewählte Applikationen wie Netscape, Acrobat Reader usw. Darüber hinaus sind natürlich weitere Software-Pakete wie z. B. Star/Open-Office installiert, diese werden derzeit aber vom ZID nicht unterstützt. Die Aktualisierung von System und Applikationen erfolgt je nach Verfügbarkeit und Sinnhaftigkeit. Bei den Windows-Applikationen wird hauptsächlich das MS Office Paket angeboten. Eine vollständige Liste aller installierten bzw. vom ZID unterstützten Programmen wird auf den Web-Seiten des ZID veröffentlicht.

Services

Die Thin Clients haben wie bisher je nach Zugangsberechtigung vollen Zugang zum Internet und den Services des ZID (UNIX Account, Mailbox, News Server, White Pages, Drucken über Copy Card). In einer ersten Testphase wird es für die Benutzer des neuen Systems keine Kernzeitbeschränkung geben.

Technische Realisierung

Nach dem Einschalten des PC-Arbeitsplatzes wird übers Netzwerk ein DHCP Server kontaktiert, der dem Client alle notwendigen Boot-Informationen (IP-Konfiguration, Bootfile und notwendige Start-Parameter) mitteilt. Danach wird je nach Methode (PXE oder Etherboot) per TFTP ein komprimiertes Image (ca. 1.5 MB) vom Boot Server geladen, welches Kernel, Netzwerktreiber und ein minimales Root Filesystem enthält. Nach Dekomprimieren und Ausführen des Kernels wird das Root Filesystem in einer wenige MB großen Ramdisk entpackt und der Init-Prozess wird gestartet. Dieser führt sofort alle notwendigen NFS Mounts durch *(/usr*, */bin*, */sbin*, */lib, ...*), startet wichtige System-Prozesse und wartet auf die User-Validierung. Diese erfolgt durch einen authentifizierten Mount des Home-Filesystems am Studentenserver per „NFS On Demand“ (s. u.). Danach werden noch einige Jobs durchgeführt (z. B. Initialisierung des User Directories, Hardware-Erkennung, Starten von Services) und schließlich wird der Desktop gestartet. Das Gerät kann jederzeit ohne weitere Aktionen einfach abgeschaltet werden.

Server

Die Redundanz der Boot Server wird dadurch bewerkstelligt, dass mehrere Server auf DHCP Requests lauschen und bei Ausfall eines Servers einfach der nächste antwortet. Die Boot-Information enthält auch eine Liste von NFS-Servern, welche für das Mounten zur Verfügung stehen. Damit kann eine Lastaufteilung, die ja eigentlich nur für NFS relevant ist, erzielt werden. Sollte allerdings ein bereits gemounteter NFS-Server ausfallen, wird der Client inoperabel und muss neu gebootet werden. Für Client-übergreifende Informationen steht noch ein Scratch Space am Boot Server zur Verfügung.

Client

Die Ramdisk des Clients, die das Root-Filesystem enthält, ist so groß gewählt, dass für */boot*, */etc, /dev* und */var* genügend Platz ist. Dafür reichen in der Regel 3-5 MB aus. */tmp* wird ebenfalls im Memory realisiert und */var/tmp* liegt am Boot Server. Da Swappen über Netz nahezu unbrauchbar ist, wird darauf verzichtet und jeder Client mit ausreichend viel Hauptspeicher ausgestattet (in Zukunft alle PCs mit 256 MB).

User Validierung

Die Benutzervalidierung geschieht nach Mounten der R/O Filesysteme und vor dem Mounten des Home-Filesystems. Im Prinzip existiert auf dem Boot Server für jeden Remote Client und jeden User ein Datensatz, der Informationen über Konfiguration und Zugriffsrechte enthält. Dadurch ist es einerseits möglich, mehrere Benutzergruppen mit verschiedenen Berechtigungsprofilen (Student, Kursteilnehmer, Tagungsbesucher) zu verwalten, und andererseits unterschiedliche Hardware Konfigurationen und Zugriffsmechanismen (Multimedia PC, Übungs PC, Kiosk PC, X-Terminal) zu ermöglichen. Im Normalfall geschieht die Validierung eines Studenten implizit durch den NFSOD Mount am Studentenserver. Es ist aber auch ein Zugriff auf andere Server bzw. per alternativem Protokoll (z. B. SMB) möglich.

Windows Applikationen

Das technische Prinzip einer Windows Terminal Session sowie die Integration in das Linux-Umfeld (Session Window, Home Directory, Drucken etc.) werden in einem separaten Artikel erläutert (siehe nächste Seite).

Security

Da es sich bei den Client PCs um UNIX-Systeme handelt, könnte ein Benutzer das System theoretisch hacken und Root-Berechtigung erlangen. Dieses „Privileg“ bringt ihm aber nicht viel und ist spätestens nach dem nächsten Reboot wieder weg. Auf alle Fälle zieht es keine Session-übergreifenden Beeinträchtigungen für den nächsten User nach sich, da dieses System ja „remote“ gebootet wird. Die Möglichkeit, dass der Client während einer Session von außen gehackt wird, und dadurch ein Datenverlust für den aktuellen Benutzer entsteht, ist sicherlich geringer als auf einem Studentenserver direkt.

Ein Problempunkt ist noch die Art und Weise, wie Home Directories gemountet werden. Da nicht 100-prozentig auszuschließen ist, dass sich doch ein User Root-Berechtigung am Client verschafft, kommt ein normaler NFS Mount nicht in Frage. Deshalb muss eine Methode verwendet werden, die auf alle Fälle eine Validierung erfordert. AFS und DCE scheiden aus administrativen und technischen Gründen aus. Bleibt eigentlich nur noch Samba, das leider einige sehr gravierende Nachteile besitzt (keine Symlinks, kein File Locking, ...). Da gerade viele der neuen KDE- und Gnome-Applikationen diese Features benötigen, kommt es sehr schnell zu einem instabilen Betrieb. Da es NFS4 noch nicht gibt, wurde eine eigene Variante (unter Verwendung von NFS3) entwickelt. Das Ganze nennt sich NFSOD (NFS On Demand) und basiert auf einem Client-Server-Mechanismus, bei dem nach einem Validierungsschritt das User Home-Verzeichnis explizit für den Remote Client exportiert wird. Dann wird per Keep-alive Mechanismus die Existenz des Clients überwacht und bei Terminierung desselbigen der Export sofort entfernt. Ein zusätzlicher Überwachungsjob verhindert die Ausnutzung möglicher Sicherheitslücken von NFS durch abgestürzte Daemons oder andere Probleme.

Ausblick

Das neue Konzept ist teilweise bereits im Zuge einer Java-Übung im Internet-Raum Favoritenstraße im Einsatz. Ende November wird der Internet-Raum FHBR2 (Freihaus, 2. Stock) zur Gänze umgestellt und es wird dort nur noch Linux zur Verfügung stehen. Danach werden schrittweise die anderen Internet-Räume dazu kommen. Hinweise und Einführungsunterlagen werden rechtzeitig im Web zur Verfügung gestellt. Die Tutoren werden auf das neue System eingeschult und geben Auskunft über unterstützte Applikationen und einfache Linux-Fragen.

Citrix Terminal Server für die Internet-Räume

Hartwig Flamm

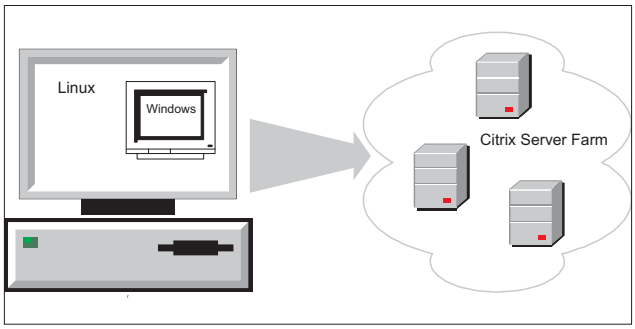
Um die Möglichkeiten der Nutzung der Internet-Räume noch vielfältiger zu gestalten, haben wir eine Citrix Server-Farm in Betrieb genommen. Sie soll es ermöglichen, beliebige Software auf den Rechnern in den Internet-Räumen laufen zu lassen, ohne dass diese für eine lokale Nutzung installiert werden muss.

Durch die Umstellung der Internet-Räume auf Linux erhält dieses Service eine besondere Bedeutung. Dadurch können auch Windows-Applikationen auf den Linux-Arbeitsplätzen genutzt werden.

Längerfristig soll es möglich sein, dass auch Institute Windows-Applikationen auf ihren eigenen Servern anbieten, die von den Arbeitsplätzen in den Internet-Räumen aus genutzt werden können.

Citrix Konzept

Die Terminal-Services auf Windows-Servern bieten die Möglichkeit, Applikationen auf einem zentralen gut ausgebauten Server ablaufen zu lassen, die Bildschirmausgabe jedoch auf einen entfernten Arbeitsplatz umzuleiten. Ein Server kann dabei eine Reihe von graphischen Logins parallel betreuen.



Citrix Terminal Session

Die Applikation wird von dem Administrator des Servers betreut. An dieser Stelle erfolgt auch die Zugriffskontrolle. Ein Arbeitsplatz kann Verbindungen zu einer Vielzahl an Servern aufbauen, sofern der Benutzer dazu berechtigt ist.

Auf dem Arbeitsplatz des Benutzers wird die Zugriffs-Software installiert. Damit können jetzt Verbindungen zu der Server-Farm definiert werden. Der Client lädt die aktuelle Liste der verfügbaren Applikationen der Farm, aus dieser wird dann die gewünschte ausgewählt. Einige Parameter wie Verschlüsselung, Farbtiefe, Audioqualität und so weiter können noch verändert werden. Bei Applikationen, die nicht für anonymen Betrieb konfiguriert sind, kann auch noch ein Benutzername eingegeben werden.

Wird die Verbindung aktiviert, so kontaktiert der Client die Farm und bekommt dort, auf Grund der Load Balancing Algorithmen, einen Server für seine Session zugewiesen. Dorthin baut er dann eine verschlüsselte Verbindung auf. Man erhält das Login-Fenster des Servers auf dem Bildschirm, es sei denn die Verbindung ist anonym oder ein Standard für Username und Passwort ist definiert.

Nach dem erfolgreichen Login werden die Laufwerke und Drucker des Arbeitsplatzes auf den Server verbunden und das Applikationsfenster wird geöffnet.

Nach dem Beenden einer anonymen Verbindung wird das temporäre Profil gelöscht.

Die Verwendung der *Metaframe XP* Software von Citrix bringt, gegenüber dem Microsoft Terminal Server, eine Reihe von entscheidenden Vorteilen. Die wichtigsten werden im Folgenden kurz dargelegt.

Citrix Lizenzvergabe

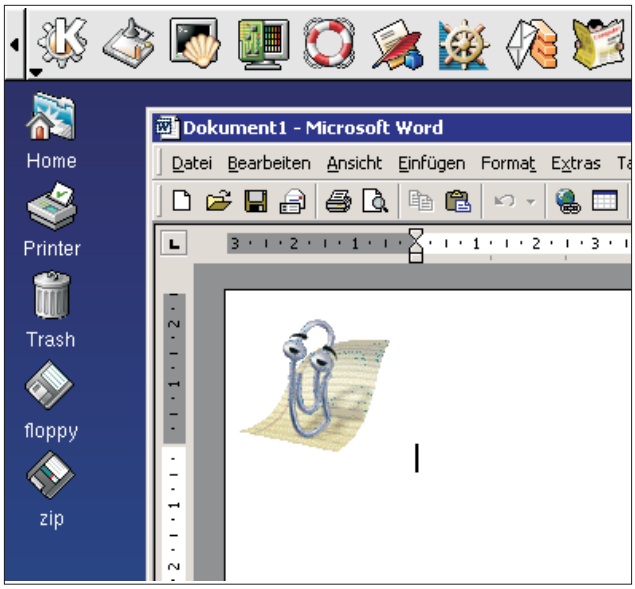
Die Zugriffslizenzen sind bei Citrix nicht an den Client sondern an den Server gebunden. Das heißt, es werden nur Verbindungen als aktiv gerechnet, die gleichzeitig auf den Server zugreifen und nicht, wie bei Microsoft, die Arbeitsplatzrechner, von denen aus eine Verbindung aufgebaut werden könnte. Ein serverseitiges

Management der Lizenzen wird dadurch erst sinnvoll möglich.

Der größte Vorteil der Citrix Software in diesem Punkt besteht aber darin, dass mehrere Server zu einem Verbund, der Citrix Server Farm, zusammengefasst werden können. Die Lizenzen können sich dann frei im Pool bewegen und dort eingesetzt werden, wo sie gerade gebraucht werden. Gemeinsam mit den „publizierten Applikationen“ und Load Balancing (siehe unten) lässt sich die Verwendung der Lizenzen sehr schön steuern.

Rahmenlose Fenster

Der Benutzer baut seine Verbindung nicht zu einem speziellen Server auf sondern wählt eine in der Citrix-Farm publizierte Applikation aus und verbindet sich zu dieser. Er wird dann zu einem der Server, welcher die gewünschte Applikation anbietet, verbunden. Der Benutzer erhält aber kein Terminal-Fenster mit dem Windows-Desktop sondern es erscheint nur die Applikation selbst, so als würde sie lokal auf dem Client ablaufen.



Word am Linux Desktop

Da dem Benutzer der Desktop nicht zur Verfügung steht, kann er auch nur die publizierte Applikation nutzen und die Ressourcen des Servers nicht einfach für andere Zwecke abzweigen.

Echtes Load Balancing

Die Aufteilung der Verbindungsanfragen auf die einzelnen Server kann durch Load Balancing Algorithmen gesteuert werden. Darin können die Anzahl der Instanzen des Programms, die maximale Netzbandbreite, CPU- oder Speicherbelegung und vieles mehr als Parameter verarbeitet werden.

Über dieses System kann der Zugriff auf einzelne Applikationen auch auf einzelne IP-Adressen oder Adressbereiche eingeschränkt werden.

Einige weitere Kleinigkeiten

Die Citrix Client Software gibt es für sehr viele verschiedene Plattformen. Neben allen Microsoft Systemen, auch DOS und PocketPC, werden auch Apple und neun UNIX-Derivate unterstützt. Die Darstellung kann mit einer Farbtiefe von bis zu 24-Bit erfolgen und die Einbindung von Sound ist möglich.

Eine Citrix Session erlaubt es, die lokalen Laufwerke und Drucker des Arbeitsplatzes am Server sichtbar zu machen. Die Applikationen können daher ihre Dokumente direkt auf das lokale Filesystem des Benutzers schreiben. Sie erscheinen am Server sogar unter dem gleichen Namen wie am (Windows-)Client. Der Benutzer hat seine Daten also immer am lokalen Rechner zur Verfügung. Ein Cut&Paste-Mechanismus ist zwischen Linux und Win-dows eingeschränkt möglich.

Mit Hilfe der Citrix Management Konsole kann die Server-Farm vom Arbeitsplatz des Administrators aus konfiguriert werden. Es können zum Beispiel Applikationen publiziert oder Load Balancing Parameter adjustiert werden. Sessions, die im System hängen bleiben, weil der Benutzer die Verbindung zur Farm verloren hat, können vor Ablauf der „Gnadenfrist“ entfernt werden.

Die ZID-Farm

Die Citrix Server Farm des ZID besteht derzeit aus drei Rechnern:

Licence-Master:
IBM Netfinity 4500
2 Pentium III 733 MHz
1,5 GB Hauptspeicher

2 Member Server:
Transtec 2400L
2 * Pentium III 1000 MHz
2 GB Hauptspeicher

Derzeit sind die zwei Java-Entwicklungsumgebungen, Forte von Sun und JBuilder von Borland, für den Übungsbetrieb installiert.

Für den Test der neuen Softwarelösung für die Internet-Räume sind vorerst Word2000, Excel2000, PowerPoint2000 und Access2000 installiert. Der IE5 aus dem Standard Windows ist ebenfalls publiziert.

Um die Problematik der Windows-Validierung zu umgehen, sind alle Applikationen für den anonymen Gebrauch publiziert. Allerdings ist die Verwendung auf den Adressbereich der Internet-Räume beschränkt. Da aber auch bei anonymen Verbindungen die beteiligten Arbeitsplätze mit geloggt werden, ergibt sich dadurch kein Sicherheitsproblem.

Im Moment stehen uns 20 Verbindungslizenzen zur Verfügung. Diese sollten von diesen drei Rechnern problemlos bewältigt werden. Wahrscheinlich ist auch eine höhere Last, also zusätzliche Lizenzen, noch ohne signifikante Beeinträchtigung des Betriebes möglich. Sollte die Nachfrage nach diesem Softwareservice massiv ansteigen, so werden allerdings zusätzliche Server nötig werden.

Sicherheit unter Linux: Packet Filter

Walter Selos

Zusätzlich zu den in der letzten ZIDline behandelten Sicherheitsmechanismen (z. B. inetd und TCP-Wrapper) gibt es für Linux noch eine generellere Methode, um den IP-Netzwerkverkehr und vor allem den wichtigen TCP-Netzwerkverkehr zu kontrollieren und bei Bedarf einzuschränken. Diese Methode heißt „Packet Filtering" und ist ein Grundbestandteil jeder Firewall. Die meisten Firewalls verfügen darüber hinaus auch über Mechanismen zur Adressübersetzung (Network Address Translation), über Proxy-Funktionalität und einiges mehr.

Jeder Verkehr über ein Netzwerk wird in Form von Paketen gesendet. Jedes dieser Pakete beinhaltet Verwaltungsinformation, den so genannten Header, und die Nutzdaten, den Body.

Im Header befinden sich Informationen über Herkunft (Source Address) und Ziel (Destination Address) des Pakets, über das verwendete IP-Protokoll (z. B. TCP, UDP, ICMP, ...) und einiges mehr (siehe IANA, *Internet Assigned Numbers Authority*, www.iana.org). Neben der reinen Datenübertragung gibt es bei verbindungsorientierten IP-Protokollen (z. B. Transmission Control Protocol (TCP)) spezielle Pakete für den Verbindungsaufbau bzw. -abbau. Auf dem TCP-Protokoll basieren die bekanntesten Services im Internet, wie z. B. HTTP (Web Traffic), SMTP (Mail-Transfer), SSH (Secure Shell) und Datentransfer (z. B. FTP).

Um auf **Paketebene** effektiv **Zugriffsbeschränkungen und Kontrollmechanismen** zu realisieren, muss man im besten Fall alle Informationen über die involvierten Protokolle haben, besonders wichtig sind aber die von den Services verwendeten Portadressen. Ebenso ist es wichtig zu wissen, welche weiteren Services zur einwandfreien Funktion eines gewünschten Services im Hintergrund noch von Bedeutung sind. Zum Surfen im Internet reicht es nicht aus, nur HTTP (Port 80) zuzulassen, man benötigt zumindest noch das Domain Name Service (DNS) mit Port 53 des UDP-Protokolls, sonst werden keine Zielknoten über deren Namen erkannt. Für ein derartiges Zusammenspiel mehrerer Protokolle gibt es zahlreiche Beispiele. Eine Liste der häufig verwendeten Protokolle (UDP und TCP) mit den zugehörigen Portadressen sind in der Datei „/etc/services" aufgelistet und können dadurch auch über den Servicenamen und nicht nur über die Portnummer spezifiziert werden.

Zur Verwendung eines Packet Filters sind also gewisse **Grundkenntnisse über den Netzwerkverkehr notwendig**, und ich möchte dringend von der Verwendung dieser Mechanismen abraten, solange man nicht wirklich weiß, was man will bzw. welche Services auf dem Rechner benötigt werden. Befolgt man diesen Rat nicht, läuft man Gefahr, sich in falscher Sicherheit zu wiegen, weil man ja ohnehin die „Firewall" aktiviert hat, ohne zu wissen, was da noch alles an den Filterregeln vorbei läuft, oder erwünschte Services funktionieren aufgrund falscher Konfiguration nicht mehr.

Zur Filtersoftware

Unter Linux werden zwei Packet Filter eingesetzt: **ipchains** für Kernels 2.2.x bzw. **netfilter/iptables** für Kernels 2.4.x.

Die Grundidee ist für beide die gleiche:
(Namen und Syntax werden hier von ipchains verwendet, für iptables sind sie leicht unterschiedlich.)

Man kann ein Muster bekannt geben und eine dafür anzuwendende Methode, hier **Target** genannt. Stimmt ein Packetheader mit diesem Muster überein, wird die Target-Methode darauf angewandt.

Targets können vordefinierte Aktionen sein, wie z. B.

ACCEPT	Paket wird weitergeleitet
DENY	Paket wird nicht weitergeleitet und einfach vergessen
REJECT	wie DENY, nur dass freundlicherweise eine ICMP-Nachricht an den Sender zurück geschickt wird, damit der Sender nicht auf ein Timeout warten muss.

Über die Funktionalität eines Packet Filters hinaus führen folgende Targets:

MASQ	kann ein privates Subnetz so verstecken, dass es als eine IP-Adresse nach außen erscheint

(dies geschieht durch Austausch der Portnummern). Da es aber nicht möglich ist, von außen eine Verbindung zu einem der dahinter versteckten Computer aufzunehmen, können solche Konfigurationen die Sicherheit wesentlich erhöhen.

REDIRECT Pakete können aus der Input-Chain (oder einer selbst definierten) an ein lokales Socket umgeleitet werden.

NAT (nur bei iptables verfügbar) die Source-Adresse bzw. die Destinations-Adresse eines Pakets kann gegen eine andere ausgetauscht werden.

Schließlich kann als Target eine selbstdefinierte komplexe „Chain" angegeben werden, in die man eine Menge von Regeln einbauen kann. Diese Technik kann man verwenden um vorzufiltern, wenn man z. B. für verschiedene Subnetze unterschiedliche Regeln (Rulesets) anwenden möchte. Es gibt bereits fix vorgegebene „Chains", z. B. *input, output* und *forward*.

Mit Hilfe von „**Policies**" kann man das Standard-Verhalten einer „Chain" festlegen, wenn keine der definierten Regeln zutrifft, also generell ablehnen (DENY) oder zulassen (ACCEPT).

Der Sicherheitsbewusste wird wohl demnach eine Deny-Policy wählen. Dabei muss man natürlich wissen, was man explizit alles erlauben muss, um einen Betrieb zu gewährleisten (siehe das oben angeführte Beispiel mit DNS, ebenso wäre z. B. zu bedenken, wenn man alles, also auch ICMP, für die Output-Chain sperrt, das Target REJECT sich genau so verhalten würde wie DENY – also wieder einmal: **Vorsicht** ist geboten !).

Beispiel für eine Filterregel

ipchains -A input -s 128.131.xxx.0/24 -d 128.131.xxx.123 www -p tcp -j ACCEPT

ipchains -A input -s 0/0 -d 128.131.xxx.123 www -p tcp -y -j REJECT -l

-A *append* (Anhängen am Ende der Kette)
-s Source Address (Absender)
-d Destination Address (Empfänger)
-p Protokoll
-j Target
-l wenn das Muster zutrifft, wird ein Eintrag ins Logfile geschrieben
-y heißt, nur SYN-Pakete (dienen zum Verbindungsaufbau für TCP) werden behandelt

Bei den oben angeführten Regeln geht es darum, den Zugriff auf den Webserver des Rechners 128.131.xxx.123 zu kontrollieren. Es soll der Zugriff nur vom eigenen Subnetz aus erlaubt sein. Die zweite Zeile ist nötig, wenn die Policy für die Input-Chain nicht auf REJECT gesetzt ist, z. B.: *ipchains -P input REJECT*

Genauere Interpretation:
1. Zeile: Alles, was vom Subnetz 128.131.xxx.0 mit der Netzmaske 255.255.255.0 (= 24 Bits) kommt und an die Maschine 128.131.xxx.123 geht, ein TCP-Paket ist und fürs WWW-Port (80, siehe /etc/services) bestimmt ist, wird erlaubt.

Wenn der Verkehr mit dem Muster nicht übereinstimmt, wird die nächste Zeile abgearbeitet. TCP-Verkehr mit beliebiger Absenderadresse und dem Ziel 128.131.xxx.123 auf dem HTTP-Port (80) wird schon beim Verbindungsaufbau (*-y*) abgeblockt und der Versuch ins Logfile geschrieben. So kann man dokumentieren, wenn jemand mit dem Web-Server von 128.131.xxx.123 Verbindung aufnehmen will, dem der Zugriff verwehrt ist.

Will man jenen Netzwerkverkehr, der einem bestimmten Muster entspricht, nur mitloggen, wird die Regel ohne Target (also ohne *-j XXXX*) aber mit der *-l* Option definiert. Das kann auch zur Verifikation und Fehlersuche sehr nützlich sein.

Dieses Beispiel soll den grundlegenden Mechanismus der Paketfilterung erläutern. Durch die Definition eigener „Chains" können sehr leistungsfähige und komplexe Filtermechanismen geschaffen werden.

Hinweise auf die Dokumentation, die Sie für einen Echtbetrieb unbedingt benötigen, finden Sie unten. Um mit den Paketfiltern sinnvoll arbeiten zu können, muss man sich doch ziemlich tief in die Materie einarbeiten, da würden „Kochrezepte" wohl nicht sehr hilfreich sein.

Zu erwähnen ist noch, dass einige Linuxdistributionen vorgefertigte Firewall-Scripts mit z. T. sehr komplexen Regeln beinhalten. Meist sind sie sehr unübersichtlich, sodass man nicht leicht Modifikationen darin vornehmen kann.

Dringende Empfehlung

Sowohl was diese fertigen Scripts betrifft als auch nach der Erstellung seiner eigenen Filterregeln, finde ich es empfehlenswert, das Filterverhalten ausführlich zu testen, um sicher zu sein, dass das, was erlaubt ist, auch wirklich funktioniert, und – wichtig für die Sicherheit – dass auch die Restriktionen voll funktionsfähig sind.

Dokumentation

1. Sehen Sie die mitgelieferten Manualpages durch: z. B.: *man ipchains* oder *man iptables*.
2. Sehr informativ sind die dazugehörigen HOWTOs, welche im Zuge des LDP (Linux Documentation Project) verfügbar gemacht wurden.

Die Links für die TU:

für *ipchains* in den HOWTOS:
http://gd.tuwien.ac.at/opsys/linux/LDP/HOWTO/IPCHAINS-HOWTO.html

für *netfilter/iptables* in Network-Administrators-Guide:
http://gd.tuwien.ac.at/opsys/linux/LDP/LDP/nag2/x-087-2-firewall.future.html

Allgemeine Information zu TCP/IP:

"The Linux Networking Overview HOWTO":
http://gd.tuwien.ac.at/opsys/linux/LDP/HOWTO/Networking-Overview-HOWTO.html

"A TCP/IP Tutorial":
http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1180.html

Wie komme ich zu meiner Campussoftware ?

Bestellung – Zugang – Installation

Andreas Klauda, Martin Holzinger

Die von der Abteilung Standardsoftware des ZID verwaltete Campussoftware steht den Instituten der TU Wien gegen einen bestimmten Kostenersatz zur Verfügung. Informieren Sie sich über das reichhaltige Angebot auf der Webseite: sts.tuwien.ac.at/css/angebot.html

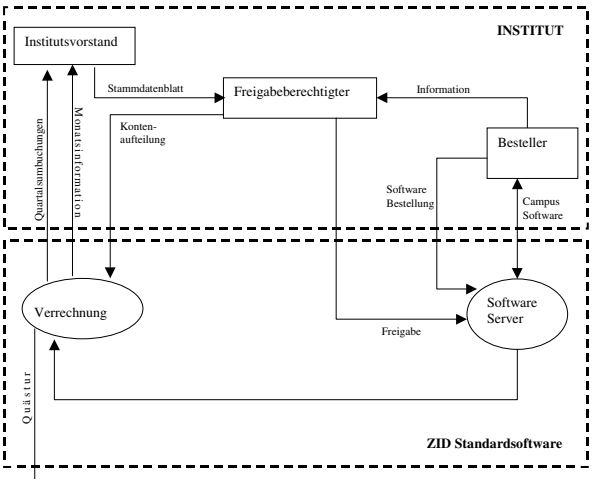
Die Campussoftware wird über den Software Distribution Server (SWD) und andere Server zugänglich gemacht, wobei jeder Lizenznehmer einen Account erhält, unter dem er auf seine lizenzierten Programme zugreifen kann.

Online-Bestellung

Wenn Sie bereits über einen Campussoftware-Account (Benutzernamen und Passwort) verfügen, können Sie neue Softwarelizenzen **online** unter

`sts.tuwien.ac.at/css/online.html`

bestellen. Diese Bestellung muss dann vom Freigabeberechtigten des Instituts online bestätigt werden. Der Besteller sollte sich mit dem Freigabeberechtigten in Verbindung setzen, da dieser **nicht** automatisch von der Bestellung verständigt wird.



Bestell- und Verrechnungsabläufe

Sollten Sie noch keinen Account besitzen, muss die erste Bestellung per Formular durchgeführt werden. Die Formulare sind auf obiger Webseite unter dem Punkt „Bestellformulare“ zu finden. Benutzername und Passwort erhalten Sie bei der ersten Softwarebestellung von uns per Hauspost.

Freigabeberechtigte müssen dem ZID bekannt gegeben werden. Das können der Institutsvorstand und/oder andere vom Institutsvorstand nominierte Mitarbeiter sein. In jedem Fall muss ein spezielles Stammdatenblatt ausgefüllt und an die Abt. Standardsoftware geschickt werden (erhältlich online als Postscript- oder PDF-File unter sts.tuwien.ac.at/css/online.html (stammdat.pdf bzw. stammdat.ps unter „Bestellformulare“) oder im Sekretariat des ZID).

Mit der Nominierung erhalten die Freigabeberechtigten das Recht, Bestellungen **online** zu bestätigen, womit diese wirksam werden. Wenn der Freigabeberechtigte schon Lizenznehmer ist, dann hat er bereits einen Account (Benutzername und Passwort) zugewiesen bekommen, der auch für das Bestätigen von Bestellungen zu verwenden ist. Andernfalls wird ihm im Zuge der Nominierung ein Account zugewiesen.

Nach der Freigabe steht die Software dem Benutzer spätestens am nächsten Tag zur Verfügung.

Bei jeder Bestellung ist auch die Wartung inkludiert. Wenn diese nicht gewünscht wird, muss sie explizit gekündigt werden (Formular wartungsende.pdf/ps), d. h. das Produkt kann in der momentan lizenzierten Version weiter verwendet werden, es können jedoch keine Updates mehr bezogen werden. Wird eine Lizenz storniert (Formular storno.pdf/ps), so muss das Programm vom Rechner gelöscht werden. Um dem gesamten Campus größere Ressourcen einzuräumen, wird ersucht, nicht mehr benötigte Lizenzen an den ZID durch Stornierung zurück zu geben.

Installation

Die Software wird für mehrere Plattformen angeboten und dementsprechend auf verschiedenen Servern zur Verfügung gestellt. Im Folgenden wird die Installation bestellter Software für Windows-, Macintosh- und Unix-Systeme beschrieben.

Windows

Die einfachste Methode unter Windows ist die Verwendung des Netzlaufwerks. Damit ist es möglich, die gewünschte Software direkt von unserem SWD-Server zu installieren, ohne vorher alle Files auf eine lokale Festplatte kopieren zu müssen (so wie früher mit FTP).

In den Dateien **`readme.1st`**, welche mit jedem Texteditor geöffnet werden können, finden Sie wichtige Informationen wie Seriennummern oder Installationshinweise.

Und so funktioniert das Ganze:

- Den **Windows-Explorer** starten.
- Im Menü ***Extras*** den Punkt ***Netzlaufwerk verbinden*** wählen.
- In der sich öffnenden Dialogbox wird automatisch das nächste freie Laufwerk angezeigt, welches bei Bedarf auch geändert werden kann. In dem Eingabefeld darunter wird folgender Netzwerkpfad eingegeben:

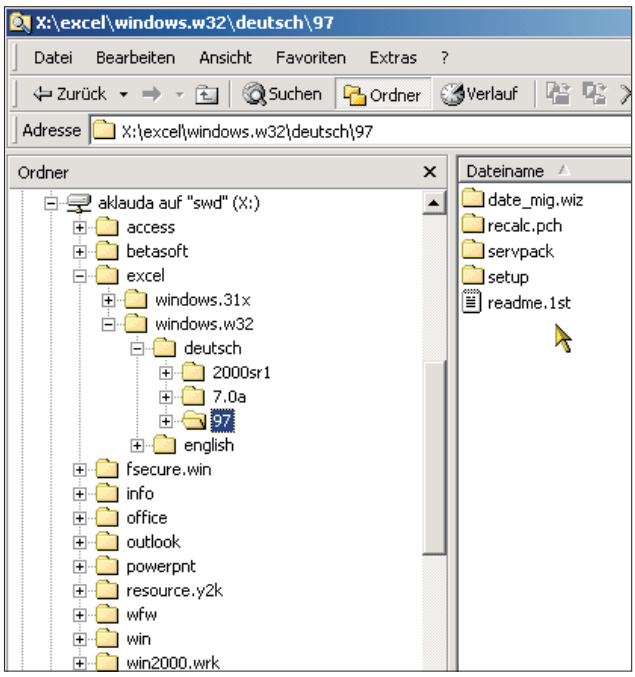
  swd***benutzername*** (z.B. \\swd\aklauda)

- Die Checkbox ***Verbindung wiederherstellen***[1] sollte deaktiviert werden.

  Im nächsten Dialog wird nach dem Passwort gefragt. Bei Windows NT/2000/XP-Rechnern gibt es noch ein zusätzliches Feld für den Benutzernamen, welches aber leer gelassen werden kann.

  Bei Windows 9x/ME Systemen sollte die Checkbox ***Kennwort speichern***[1], aus Sicherheitsgründen deaktiviert werden.

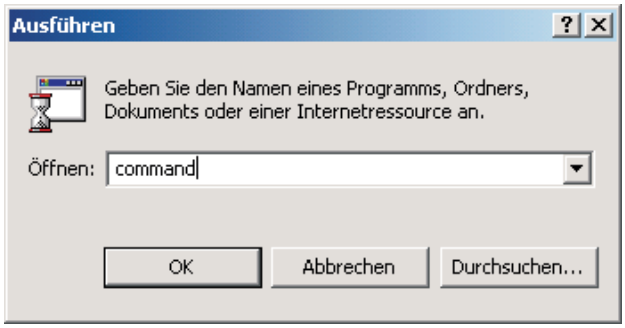
  In dem nun vorhandenen Netzlaufwerk sind alle lizenzierten Programme sichtbar, z. B.:



Die WWW-Direktinstallation (TUINST) und die Home-Verzeichnisse über den Webbrowser stehen nicht mehr zur Verfügung, da die Installation über Samba (Netzlaufwerk) einfacher ist und das Service kaum mehr verwendet wurde.

Sollten Sie **keine Verbindung** zum SWD-Server herstellen können, sind folgende Dinge zu beachten:

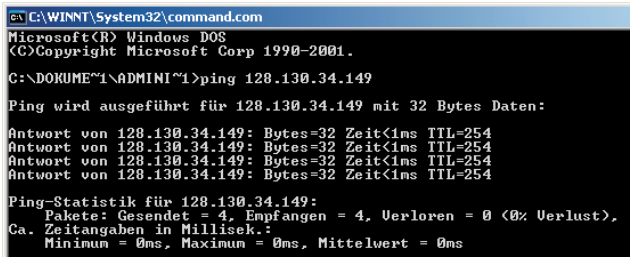
1. Ihr Netzwerk muss richtig konfiguriert und verkabelt sein.
2. Ihr Rechner muss angemeldet sein und einen gültigen DNS-Eintrag haben (Anmeldung: http://nic.tuwien.ac.at/tunet/anmeldung.html).
3. Mit dem Befehl **`ping`** und der Angabe der IP-Adresse des Software-Servers kann überprüft werden, ob der SWD-Server erreichbar ist (Eingabe **`command`** über ***Start***-Menu – ***Ausführen***):



Dann öffnet sich ein DOS-Fenster, dort geben Sie **`ping 128.130.34.149`** ein.

[1] Der genaue Wortlaut variiert je nach Betriebssystem

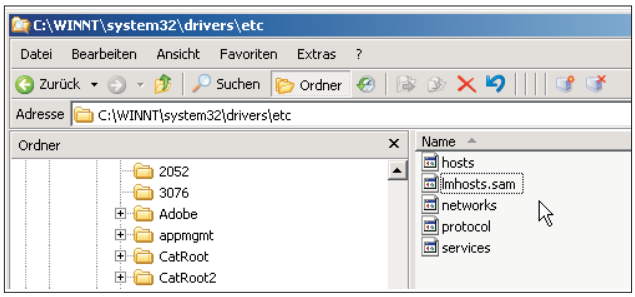
Eine positive Rückmeldung des SWD-Servers ist in folgendem Bild ersichtlich:



Auf einigen Rechnern ist noch ein Eintrag in der Datei **LMHOSTS** notwendig, dieses finden Sie auf

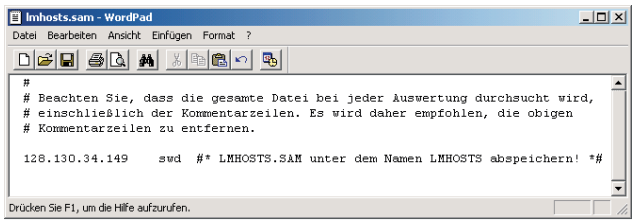
Windows 9x/ME-PCs im Systemverzeichnis (z.B. C:\windows),

Windows NT/2000/XP-PCs im Systemverzeichnis \system32\drivers\etc (z.B. c:\winnt\system32\drivers\etc).

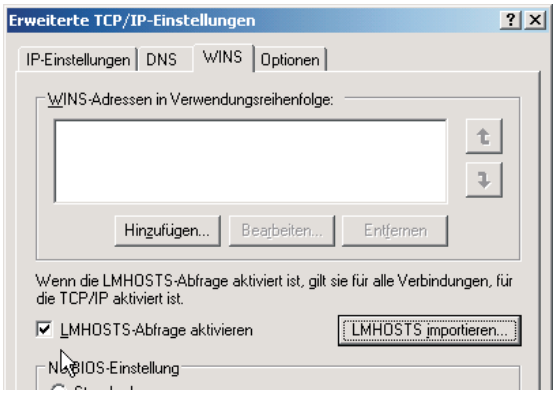


Eventuell hat die Datei die Endung **SAM**. In diesem Fall muss sie zu **LMHOSTS** (ohne Punkt) umbenannt werden. Danach kann sie mit einem Texteditor (z.B. Notepad) geöffnet werden, um folgende Zeile hinzuzufügen:

```
128.130.34.149   swd
```



Eventuell ist die Aktivierung der LMHOSTS-Abfrage über ***Netzwerkeigenschaften / LAN-Verbindung / Eigenschaften*** des TCP/IP-Protokolls über die WINS-Registrierkarte notwendig:

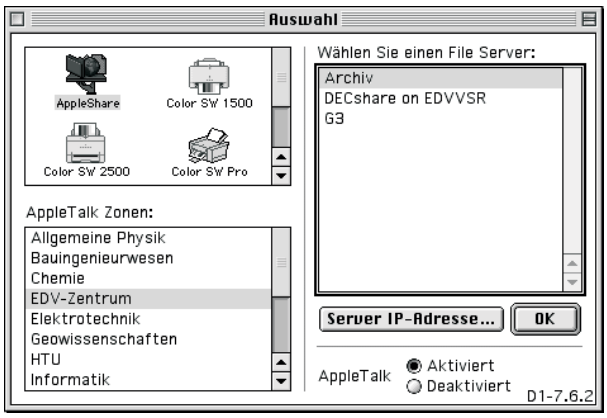


Ein Neustart ist im Normalfall nicht notwendig. Danach sollte eine Verbindung möglich sein.

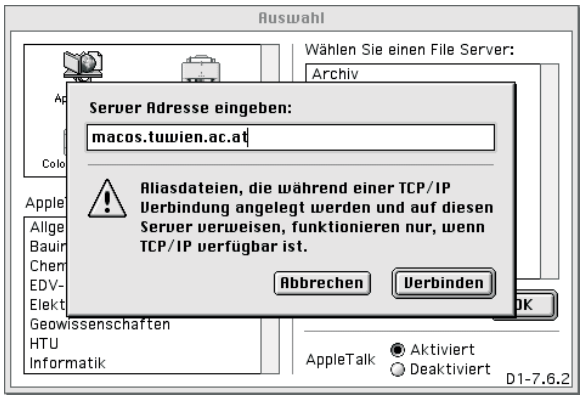
Macintosh

Zugangswege sind:

- AppleShare über AppleTalk:
  „Archiv“ in der Zone „EDV-Zentrum“



- AppleShare über TCP/IP:
  „Server IP Adresse ...“ macos.tuwien.ac.at
  Voraussetzung ist zumindest System Software 7.5.3, Open Transport 1.1.2 und AppleShare Client 3.7.2.
  Dieser Weg bietet einen etwas höheren Durchsatz als AppleShare über AppleTalk.



- http://macos.tuwien.ac.at/Archiv/
  Dieser Weg erlaubt keine Direktinstallation vom Server. Außerdem wird Ihr Passwort im Klartext übertragen. Der Zugriff auf große Dokumente kann sehr lange dauern.

UNIX

Der Zugang zum SWD-Server über FTP, welcher für die meisten UNIX-Programme verwendet wird, bleibt weiterhin erhalten und wird demnächst durch ein Secure FTP ergänzt, das eine sichere (verschlüsselte) Übertragung der Daten ermöglicht.

Für Campussoftware-Produkte für UNIX-Plattformen gibt es je nach Produkt unterschiedliche Zugangsmechanismen. Am SWD-Server ist entsprechende Dokumentation in den `readme`-Files vorhanden.

Der neue Software Distribution Server SunFire 3800

Helmut Mastal, Werner Steinmann

Der neue Software-Server SunFire 3800 steht kurz vor der Inbetriebnahme als Hauptsystem für die Verteilung der Campus-Software der TU Wien. Damit wird das symmetrisch-redundante Doppelsystem von Sun Enterprise 450 Servern sukzessive abgelöst, und es kommt mittelfristig zu einer Konfiguration mit innerer Redundanz und einem höheren Anteil an aktiven Komponenten.

Entwicklung des Software Distribution Servers in den letzten drei Jahren

In den Jahren 1997/98 wurden zuletzt die Systeme des Software Distribution Servers neu installiert, indem eine SPARCstation 20 durch 2 gleiche, redundante Systeme Sun Enterprise 450 mit je 2 296 MHz Prozessoren und je 512 Mbyte Memory ersetzt wurde. Die SPARCstation 20 hatte bereits 3 Jahre zuvor eine noch ältere Sun Maschine (SPARCstation 330) abgelöst. Die beiden 450 Systeme, die also schon die 3. Generation der Software Distribution Server darstellten, bildeten ein symmetrisches Active-Standby Paar. Zur Vorrätighaltung der zu verteilenden Campus-Software dienten zwei StorageWorks RAID-Systeme mit netto ca. 500 Gbyte Speicherplatz bei den damaligen Plattengrößen. An Software wurde angeboten: Anwendungssoftware für PC und Unix sowie Betriebssysteme für PC. Gleichzeitig wurde die Administrationssoftware SDS (Software-Distribution-System) laufend weiter entwickelt und verfeinert, mit der die Validierung der Benutzer und die Zuordnung der in Sublizenzen vergebenen Software-Pakete ermöglicht wird. Den Benutzern steht die Software über die Services FTP, Samba und HTTPS zur Verfügung. Der Zugang über SFTP wird derzeit in Erwägung gezogen.

Erfreulicherweise entwickelten sich der Software-Server und die Akzeptanz seiner Dienstleistungen sehr gut. Es war in den letzten Jahren mit einem zehnprozentigen jährlichen Zuwachs bei der Anzahl der Software-Downloads zu rechnen. Der Speicherplatzbedarf für Campus-Software stieg aber wegen der zunehmenden Komplexität der Software-Pakete und höheren Spezialisierung bis zu 40 Prozent pro Jahr. Dieser Zuwachs konnte zeitweise nur durch eine rigorose Politik bei der Zurverfügungstellung alter Software-Versionen bewältigt werden.

Es ist daher nicht verwunderlich, dass bald nach der Installation der Enterprise 450 Servergeneration Überlegungen über die nächste Innovation angestellt wurden. Dabei bildete sich folgende Zielvorstellung heraus: Nach Erreichung des Endes des Lifecycles der 450 sollte ein Server/Speicher-System zur Verfügung stehen, das in der Lage war, wesentlich größere Datenmengen (Terabytes) vorrätig zu halten, und das auch leistungsfähig genug war, die notwendigen seriellen Batch-orientierten Operationen (Backup, Linken der den Benutzern zugewandten Verzeichnisse mit den gespeicherten Daten) in einer vernünftigen Zeit durchzuführen. Auch sollte diese Leistung dadurch erbracht werden, dass ein höherer Anteil der Gesamtressourcen aktiv dem Benutzerbetrieb zur Verfügung steht als bisher.

Mit diesem Szenario als Ziel wurden bereits in den Jahren 1999 und 2000 Investitionen getätigt, die unmittelbare Entlastungen bei den vorhandenen 450 Systemen bringen sollten, aber auf jeden Fall auch in das Gesamtkonzept der nächsten Servergeneration ab 2001/2002 passen mussten. In diesem Sinne wurden im Herbst 1999 zwei Bandwechselsysteme (Jukeboxes) vom Typ Overland LibraryXpress mit je 15 Slots für Backup-Zwecke angeschafft, die das vorhandene DLT 7000 Laufwerk ablösten und in ihrer Kapazität bis zu ca. 1 Terabyte Daten ausreichen werden. Im Frühjahr 2001 wurde schließlich die Backup-Maschine SPARCstation 20 (SWD-Server der 2. Generation) durch eine Sun Enterprise 450 abgelöst und damit die Performance der Server-Backups verbessert.

SWD 1. Generation
SPARCstation 330 (hinten)
plus Plattengehäuse

SWD 2. Generation
SPARCstation 20

SWD 3. Generation
Sun Enterprise 450

SunFire 3800:
Gesamtansicht

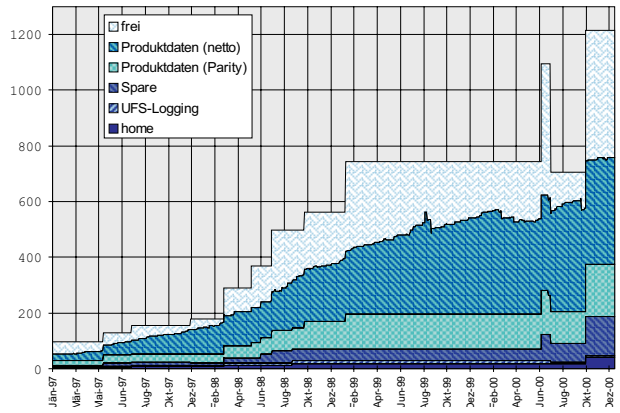
SunFire 3800:
Fronttüre geöffnet
sichtbar
(von oben nach unten):
RAID T3
Domain Controller
CPU/Memory Board
cPCI Interface Karten
redundante Stromanschlüsse

Altes StorageWorks
RAID-System 450

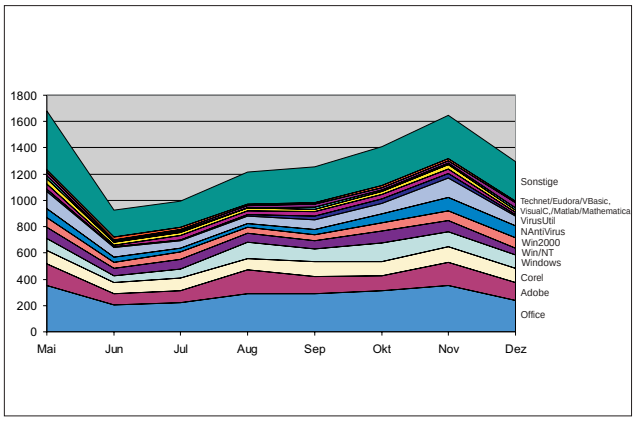
Neues MetaStor
RAID-System 3702

2 Overland
Bandwechselsysteme
+ Sun Enterprise 450

Die wesentliche Erneuerung im Jahr 2000 war der Übergang zu einer neuen Generation von Speichersystemen. Es wurde das MetaStor RAID-System 3702 angeschafft, das mit heutigen Plattengrößen (73 Gbyte) bis zu 2 Terabyte (netto etwa 1.5 Terabyte) sinnvoll ausbaubar ist und paarweise redundante Verbindungen zu jedem Host in Fibre-Channel Technologie mit Gigabit-Übertragungsraten ermöglicht. Das RAID-System 3702 ist damit als SAN (Storage Area Network) anzusprechen und hat mit einem Lifecycle von etwa 5 Jahren genau so in die bestehende vollredundante Konfiguration der 450er zu passen wie in die Endkonfiguration mit innerer Redundanz, die voraussichtlich 2002/2003 erreicht werden wird.



Übersicht RAID-Belegung (GB)
1. 1. 1997 bis 31. 12. 2000



SWD-Downloads im Jahr 2000
nach Produktgruppen

Erfahrungen aus der bisherigen Struktur

Die bestehende, aus den Jahren 1997/98 stammende Servergeneration ist als symmetrische, hoch redundante Lösung anzusehen, mit den beiden Sun Enterprise 450 Systemen als 100-prozentiges gegenseitiges Backup, während die beiden alten (jetzt schon außer Betrieb genommenen) StorageWorks RAID-Systeme für einen sinnvollen Benutzerbetrieb stets gleichzeitig benötigt wurden. Hochredundante Lösungen können folgende Probleme in sich bergen: einerseits sind möglicherweise Komponenten doppelt ausgeführt, die nie oder sehr selten (innerhalb des Lifecycles von etwa 3 Jahren) Fehler aufweisen, andererseits können gerade in hochredundanten Konfigurationen sehr leicht neue Single-Points-of-Failure entstehen (oder übersehen werden), allein dadurch, dass die Verbindungen zwischen den einzelnen Redundanzebenen nicht mit der erforderlichen 4fach-Redundanz ausgeführt sind.

Die vollständige Redundanz für ein Service bewirkt, dass höchstens die Hälfte aller vorhandenen Ressourcen produktiv genutzt werden kann, während der Rest nur darauf wartet, dass irgendeine aktive Komponente ausfällt. Auch in der ursprünglichen Sun 450 Konfiguration gab es solche versteckte Single-Points-of-Failure: das waren das ATM-Interface für den Benutzerzugang, sowie die für beide Systeme gemeinsame USV (unterbrechungsfreie Stromversorgung), die nur einen einzigen Stromkreis unterstützte. Alle diese versteckten Probleme konnten mit geringen Mitteln noch für die alten 450 Systeme behoben werden und für die Neuplanung entsprechend berücksichtigt werden (nur 100 Mbit/s Ethernet-Interfaces, zwei Stromkreise einer neuen Emerson USV (von Liebert Hiross) dediziert für den Software-Server). Untersucht man die tatsächlich aufgetretenen Takeovers, also die fehlerbedingten Wechsel von einem System zum anderen, so findet man etwa ein Takeover pro Monat im Durchschnitt, wobei aber die Mehrzahl zu Lasten der alten USV geht, jedoch kein einziger Fall auf ein permanentes Hardware-Problem bei den Serversystemen zurück zuführen ist.

Planung des neuen Servers SunFire 3800

Schon bei den ersten Planungen für das neue Softwareserver-System war klar, dass bei einem System, das Services für den gesamten Campus 24 Stunden pro Tag über das Netz anbietet, nie wirklich auf Redundanz verzichtet werden kann. Es sollte aber bei allen Komponenten, insbesondere bei den teuren Ressourcen wie Prozessoren und Speicher genau abgeschätzt werden, ob eine 100-prozentige Redundanz wirklich notwendig und sinnvoll ist, und ob nicht Redundanz in geringerem Ausmaß eine genügend hohe Verfügbarkeit liefert. Es ergab sich daraus in der Folge die Forderung, dass von den kritischen, teuren Ressourcen mindestens zwei Drittel aktiv für den Normalbetrieb zur Verfügung stehen sollen, und höchstens ein Drittel als Hot-Standby bereit gehalten wird.

Da im heurigen Frühjahr die SunFire Servergeneration als Nachfolgeserie der Sun Enterprise Generation auf den Markt kam, wurden Lösungen, die Redundanz in einem bestimmten Ausmaß vorsehen, durch das in der SunFire Serie ab dem Modell 3800 vorhandene Domainkonzept sehr begünstigt. Dieses baut auf innere Redundanz auf und kann Ressourcen im Verhältnis von Prozessor/Memory-Boards aufteilen. Da es schließlich gelang, einen SunFire Server 3800 mit 4 Sparc III Prozessoren und 4 Gbyte Memory zu einem unschlagbar günstigen Einführungspreis von Sun Austria zu erwerben, war der weitere Weg klar: Neben der SunFire 3800 als aktivem Server

bleibt zunächst eine der Sun 450 mit einem auf 2 Gbyte erweiterten Hauptspeicher als Hot-Standby Server erhalten. Zu einem späteren Zeitpunkt wird unter Ausnützung des Domainkonzepts die SunFire 3800 um eine zweite Domain mit nur 2 Prozessoren erweitert, sodass dann wieder zwei Drittel des Gesamtsystems aktiv bleiben. Das zweite alte Sun Enterprise 450 System bleibt (wie die meisten älteren Software-Server-Systeme) produktiv erhalten und wird in Zukunft als neuer Goodie-Domain-Server eingesetzt werden.

Installation und Konfiguration des neuen Servers

Hardware

Die drei vorhandenen Sun Ultra Enterprise 450 Server werden Schritt für Schritt durch eine Sun Fire 3800 mit zwei Domains ersetzt. Mit der SunFire 3800 verlagert sich die Redundanz durch mehrere getrennte Maschinen auf die Ausfallssicherheit innerhalb eines Gehäuses, wobei weiterhin eine Cluster-Konfiguration mit Failover betrieben wird. Momentan besteht der Cluster aus einer Sun Ultra Enterprise 450 und einer SunFire 3800 mit einer Domain.

Die Begriffe Domain und Partition verwendet Sun in diesem Zusammenhang zur Beschreibung verschiedener Konfigurationsmöglichkeiten ihrer SMP Server. Diese Konzepte wurden mit der Sun Enterprise 10000 (Starfire, mit bis zu 64 UltraSPARC-II Prozessoren und 64 Gigabyte Hauptspeicher) populär und sind in der SunFire Serie weiterentwickelt worden.

Eine Sun Enterprise 450 ist schon seit einiger Zeit dediziert als Backup-Server mit Legato NetWorker im Einsatz. Das Backup großer Datenmengen ebenso wie das Einspielen läuft weitgehend über ein eigenes internes Netzwerk und nicht über die vom offiziellen TUNET erreichbaren Anschlüsse.

Eine weitere E450 wird nun für gd.tuwien.ac.at frei; generell wird in all unseren Plänen einer sinnvollen Nutzung für wiederverwertbare Teile hohe Bedeutung beigemessen. Und die dritte – zurzeit im Cluster befindliche – 450-er dient dem Testen und Entwickeln von Software bzw. als Ersatz bei Problemen.

Die bisherige Variante mit mehreren Maschinen war kostenneutral zu einem brauchbaren Wartungsvertrag und gab uns mehr Flexibilität bei Entwicklung und Testen. Bei der neuen Maschine ist ein Wartungsvertrag im Bundle dabei.

Die Sun Enterprise 450 Systeme sind jeweils mit 2 x 296 MHz UltraSPARC-II Prozessoren, mindestens 1 GB Memory, redundanten Netzteilen, Lüftern, SCSI-Controllern, Fibrechannel-Controllern, Ethernet- und ATM-Anschlüssen ausgestattet. Es gab seit ihrem Einsatz keine Totalausfälle der Maschinen sondern eher nur Standardsituationen wie Platten- oder Memory-Tausch. Die heiklen ATM-Anschlüsse haben sich nicht bewährt und wurden durch Fastethernet-Controller ersetzt, die absolut problemlos funktionieren und als Vierfachanschlüsse auch sehr kostengünstig sind.

Die neue Sun Fire 3800 hat ein CPU Board mit 4 GB Memory und 4x750 MHz UltraSPARC III CPUs (d. h. eine Domain/Partition). Sie ist mit einem Sun StorEdge T3 RAID und einem Media Tray D240 in einem Sun Fire Systemschrank eingebaut, wobei bezüglich Ausfallssicherheit gegenüber unserer bisherigen Konfiguration schon im Design viele Vorkehrungen getroffen sind und man nicht den Eindruck von Add-ons hat. Sogar die PCI Karten sind im Betrieb tauschbar, sie sind als cPCI (compact PCI) ausgeführt. Dieser Kartentyp ist aber (noch) nicht sehr weit verbreitet und falls man ganz bestimmte Karten wie für die Fibrechannel-Anbindung der verwendeten MetaStor RAIDs sucht, ist das langwieriger als die Verwendung gängigerer Interfaces. Das CPU Board ist in unserer Konfiguration natürlich nicht sinnvoll im Betrieb zu wechseln, sondern erst wenn ein zweites als zweite Domain vorhanden wäre. Im Betriebssystem bzw. im Domain Controller ist entsprechende Unterstützung der Hardware vorgesehen, es lassen sich z. B. CPUs und Interfaces aktivieren/deaktivieren.

Software

Bei der Software-Liste ist Einiges bereits durch die verwendete Hardware vorgegeben:

Als Betriebssystem für die neue Anlage ist Solaris 8 ab Release 4/01 notwendig, d. h. z. B., dass wir alle eingesetzte Software auf 64-Bit-Tauglichkeit überprüfen mussten. Auf der älteren Anlage war noch Solaris 2.6 in Verwendung (nach Version 2.6 wurde mit 7 bzw. jetzt aktuell 8 weitergezählt). Unserer Anforderung nach möglichst weit verbreiteter Software entspricht Solaris immer noch, obwohl sich in den letzten Jahren die Verbreitung verschiedener Unix-artiger Betriebssysteme stark geändert hat. Die unter diesem Betriebssystem vorhandene Programmierumgebung ist uns vertraut, wobei wir dabei wesentlich auf das GNU Project und andere frei verfügbare Programme zurückgreifen und nicht nur Produkte von Sun einsetzen. Die von Sun mitgelieferten Versionen von Perl etc. sind oft nicht die Versionen, auf die unsere Verteilungsmechanismen aufbauen, und müssen ergänzt werden. Auch bei der Programmierumgebung gab es unter Solaris 8 nicht nur einen Namenswechsel auf Forte statt bisher Workshop. Adaptierungen der Verteilungsmechanismen über TCP/IP oder andere an der TU gewünschte Protokolle sollten aber keine ernsthaften Probleme bereiten.

Als Cluster-Software mit Failover-Eigenschaften wählten wir nach unseren bisherigen Erfahrungen wieder das Produkt Watchdog der Firma Apptime (ehemals Firma Wizard) in München, das unseren Anforderungen (KISS – *keep it small and simple*) entspricht (siehe: www.apptime.de). Das von Sun selbst angebotene Cluster Environment ist ausschließlich auf Sun-Produkte konzentriert und wäre schon aus diesem Grund für unsere Konfiguration nicht sinnvoll einsetzbar.

Als Backup-Software verwenden wir Solstice Backup Version 6.0.1 (= Legato NetWorker), wobei wir zurzeit 35 Clients auf einem eigenen Backup Server unterstützen (Sun Enterprise 450 mit 2 Overland DLT Juke Boxes).

Im Falle eines GAUs wäre mit einer Woche zu rechnen, bis Hunderte von GigaBytes wieder von den Bändern restauriert sind.

Zur Unterstützung von Filesystemen, Volumes, dem Verändern von Filesystemen im Betrieb (*Growfs*), *Transaction Tracking* (*Journaled File Systems*) und zum Aufsetzen unserer Verteilungs-Software verwenden wir weiterhin Online DiskSuite Version 4.2.1 (ODS) unter Solaris. Dieser betriebssystemnahe Software-Teil ist insofern kritisch, als auch hier die Umstellung von Solaris 2.6 bzw. 7 auf 8 zum Tragen kommt. Ein Übergang auf Veritas Produkte, die von Sun für seine eigenen Cluster-Lösungen verwendet und angeboten wird, war bisher nicht notwendig, denn ODS wird entgegen anders lautenden Ankündigungen weiterhin unterstützt und ist für unsere Bedürfnisse ausreichend.

Das bereits vorhandene Notification System (Mail, SNMP, Pager, Auswerten von Logs) wird kontinuierlich weiter verbessert, wobei auf entsprechende Unterstützung bei den neueren Komponenten geachtet wurde. Die Monitoring Services bei der USV oder Ambiental Monitoring bei den Suns sind wesentliche Verbesserungen gegenüber der alten Anlage.

Um mit der Entwicklung bei den Konsolen für Server (Domain Controller) oder RAID Schritt zu halten, haben wir ein neues, rein administratives 10 MBit/s Netzwerk eingeführt. Das Sun T3 RAID hat einerseits bereits gar keine serielle Konsole mehr, andererseits sind zur Konfiguration über Ethernet nur unsichere Protokolle wie Telnet und Ftp vorgesehen. Bei Netzwerkdruckern ist diese Art von Konfiguration im schlimmsten Fall wahrscheinlich höchstens lästig, aber kein Desaster wie eine gestörte Konfiguration bei einem RAID. Die Steuerung der StorageWorks RAIDs basierte noch auf einem offensichtlich proprietären Betriebssystem der Firma Digital, der Domain Controller, das T3 und die MetaStor RAIDs bauen hingegen auf bekannten *embedded* UNIX-Systemen wie VxWorks oder pSOSystem auf. Das Ansprechen der RAIDs zur Konfiguration über den SCSI-Bus ist aber erst nach einer Grundkonfiguration im Console Mode möglich oder andere elementare Funktionen wie Firmware Upgrade sind (sinnvollerweise) nur so vorgesehen.

Ausblick und zukünftige Services

Die Vollinbetriebnahme der SunFire 3800 ist mit dem Zusammenschluss mit dem RAID-System 3702 noch im November diesen Jahres geplant und möglicherweise bei Erscheinen der ZIDline bereits abgeschlossen. Die Benutzer am Campus der TU Wien sollten davon nicht allzu viel merken. Auch die Services des neuen Servers werden weiterhin über den generischen Hostnamen *swd.tuwien.ac.at* angesprochen. Nach der Inbetriebnahme ist daran gedacht, SFTP (Secure FTP) als neues Service anzubieten, insbesondere aber nicht ausschließlich für Unix-Benutzer, da das alte FTP keine verschlüsselte Übertragung kennt, Samba-Clients im Unix-Bereich aber nicht sehr verbreitet sind (vergl. auch den Artikel „Wie komme ich zu meiner Campussoftware ?“ auf Seite 21).

Referenzen

Für den allgemeinen Überblick ein Buch von:
Adrian Cockcroft and Richard Pettit, Sun Performance and Tuning, Sun Microsystems Press, Second edition, 560 pages, ISBN 0-13-095249-4

Ältere Artikel zum Software Dstribution Service an der TU Wien sind im Archiv der Ausgaben von Zeitschriften des ZID nachzulesen:
www.zid.tuwien.ac.at/zidline/archiv.html

Für aktuelle Informationen einige Web Pages der Hersteller im Internet bzw. Software Server zur verwendeten Software auf swd.tuwien.ac.at, z. B. sind die Manuals für Sun Systeme über deren Homepage oder direkt unter docs.sun.com zu finden:

Sun Microsystems, white papers, manuals, patches:
www.sun.com
SunFire 6800/4800/3800 Systems Overview Manual

Overland Data DLT juke boxes: www.overlanddata.com

LSI Logic - Metastor RAID: www.lsilogic.com

JNI - fibre channel adapter: www.jni.com

Apptime - Watchdog Cluster Software: www.apptime.de
Apptime Watchdog Service Cluster System Adminstration Handbook, Juli 2001

The Apache Software Foundation, Web Server:
www.apache.org

Samba Web Pages, Samba Server (Netbios over TCP/IP):
www.samba.org

aufbereitete Solaris Freeware: www.sunfreeware.com

Liebert Hiross Emerson USV: www.liebert-hiross.de

Peter Pawlak, „Five Nines“ – Is It Even Possible ? Directions on Microsoft UPDATE, Juni 2001

Datenerfassung und –auswertung mit LabVIEW im Laserlabor des Instituts für Allgemeine Physik

Reinhard Schnitzer und Wolfgang Husinsky
Institut für Allgemeine Physik, Technische Universität Wien
e9625636@student.tuwien.ac.at, husinsky@iap.tuwien.ac.at

Seit kurzem ist das Programm LabVIEW auch als Campuslizenz für Institute der TU Wien erhältlich. Für TU-Studenten gibt es eine Studentenlizenz. LabVIEW ist eines der bekanntesten Programme zum Erstellen von Applikationen für die Steuer- und Messtechnik, mit einer produktiven graphischen Programmierumgebung. Der folgende Artikel beschreibt mehrjährige Erfahrungen mit LabVIEW in der Experimentsteuerung.

Warum LabVIEW ?

Am Institut für Allgemeine Physik wird LabVIEW seit etwa 10 Jahren im Laserlabor für die Steuerung von Experimenten genutzt. Zum damaligen Zeitpunkt war der Einsatz dieser neuartigen Programmiersprache (eigentlich besser Programmierumgebung) noch ziemlich exotisch und wurde von vielen mit Misstrauen (in etwa als Spielerei) betrachtet. Letzter Anstoß, LabVIEW generell für unser Experiment zur Steuerung, Datenerfassung und teilweise auch Datenauswertung zu verwenden, war folgendes Ereignis: Wir verwendeten zum damaligen Zeitpunkt eine PDP 11 zur Steuerung und Datenerfassung und die Programme waren in Assembler und Fortran geschrieben und liefen unter einem „ernst zu nehmenden“ Betriebssystem. Wir hatten damals im Wesentlichen als Verdienst des Dissertanten P. Wurz gut funktionierende Treiber für unsere GPIB (IEEE)-Interface-bestückten Geräte. Für ein neues Tektronix Digital-Oszilloskop sollte einfach die gespeicherte Kurve ausgelesen und abgespeichert werden. Versuche, unsere GPIB Treiber zu adaptieren und zu verwenden, scheiterten im Wesentlichen daran, dass offensichtlich eine Inkompatibilität zwischen dem IEEE Interface des Oszilloskops und der PDP trotz wochenlanger Versuche auch der Experten nicht zum Ziel führte. Tests bei der Firma Tektronix zeigten, dass das Interface des Scopes nicht defekt war. Schließlich versuchten wir auf einem damaligen MacII und der Ur-Version von LabVIEW, die wir dafür anschafften, das Problem zu lösen. Innerhalb eines Vormittags hatten wir ein funktionierendes Programm zum Datenerfassen und einfachen Steuern des Digitalscopes. Darauf hin beschlossen wir, RSX auf einer PDP für die weitere Datenerfassung und Steuerung in unserem Labor ein gutes Betriebssystem sein zu lassen und auf Macintosh mit LabVIEW umzustellen.

Seither verwenden wir ausschließlich LabVIEW im Laserlabor für verschiedenste Zwecke (eine kurze Übersicht folgt weiter unten) und auch andere Gruppen am Institut setzen heute LabVIEW ein. Ursprünglich hauptsächlich auf MacOS Systemen laufend, hat sich LabVIEW auch als Standard auf Windows-Systemen etabliert.

Charakteristika von LabVIEW

LabVIEW ist eine graphische Programmiersprache (sowohl die Benutzeroberfläche ist dabei ein Abbild eines Gerätes als auch die Programmierung selbst erfolgt graphisch), die ursprünglich dazu gedacht war, Daten von analogen und digitalen Quellen komfortabel zu erfassen, nachzubearbeiten und zu speichern. Dabei ist es das Ziel, ein „virtuelles Gerät“ (mit Schaltern, Zeigern etc.) zu erstellen. Ein großer Vorteil, der sich bei der Verwendung von LabVIEW zwangsweise ergibt, ist diese graphische, anschauliche Methode, aber vielleicht noch wichtiger, die dabei phantastisch einfache und direkte

Art, mit verschiedensten Datentypen und Datenströmen, wie sie aus Messgeräten kommen, zurechtzukommen. Jeder, der einmal die Datenerfassung eines einfachen Gerätes mit Assembler durchgeführt hat (man denke nur an die Behandlung von Floatingpointzahlen), wird das schätzen. Es hat sich gezeigt, dass dies in einem Universitätslabor besonders vorteilhaft ist, da auch Studenten, die nicht Experten in Datenverarbeitung sind, relativ leicht früher erstellte Programme verstehen und adaptieren sowie in kurzer Zeit eigene erstellen können.

Als Konsequenz hat man nicht mehr seitenlangen „Spaghetticode“ sondern eine halbwegs übersichtliche graphische Benutzeroberfläche, die auf einen Blick verrät, was das Programm macht. Die unterschiedlichen Variablentypen sind durch verschiedene Farben der Verbindungsleitungen gekennzeichnet und sind daher leicht zu unterscheiden. Im Vergleich zu traditionellen Programmiersprachen wie C, C++, Fortran und ähnlichen, ist es bei LabVIEW nicht notwendig, den gesamten Text zu lesen, denn man hat das ganze Programm wie ein Bild vor sich.

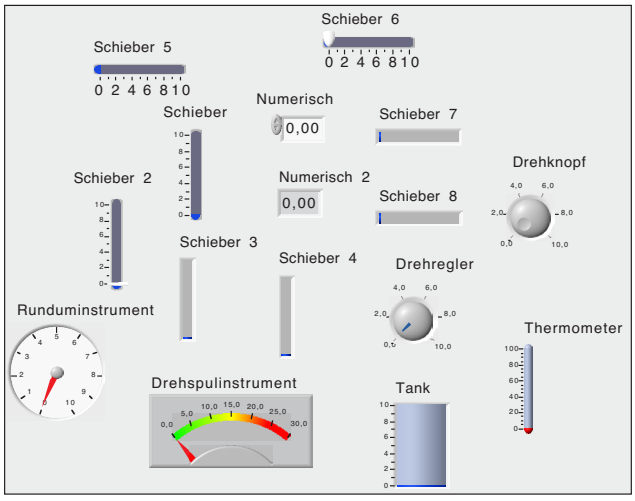
Das Programmieren in LabVIEW hat eine Ähnlichkeit mit dem Entwickeln einer elektronischen Schaltung. Die einzelnen Variablen können in einer graphisch ansprechenden Benutzeroberfläche durch Schalter oder mit Hilfe der Tastatur eingegeben werden. Je nachdem, ob es sich um eine Boolesche Variable, einen String, eine Integer oder Real-Zahl handelt, gibt es verschiedene Möglichkeiten der Eingabe. Für eine Zahl zum Beispiel hat man verschiedene Drehknöpfe, für eine Boolesche Variable existieren verschiedene Arten von Schaltern, die True/False Zustände. Genauso umfangreiche Eingabemöglichkeiten gibt es auch für den Variablentyp String.

In Abbildung 1 sind einige Ein- und Ausgabeelemente abgebildet. Ähnlich funktioniert auch die Ein- und Ausgabe von Booleschen Variablen. Man sieht aber schon an dieser Stelle die Vorteile von LabVIEW. Es ist keine lange Einarbeitungszeit notwendig, um ein Virtuelles Messinstrument mit einer übersichtlichen Benutzeroberfläche zu gestalten. Ähnlich einfach ist es auch, die einzelnen Eingabewerte, die so genannten „Controls“, die in der Abbildung 1a zu sehen sind, mit den virtuellen Ausgabegeräten, den so genannten „Indicators“, zu verbinden. Dies ist in Abbildung 1b zu sehen. Allerdings ist dies hier nur zur Demonstration gedacht. In Wirklichkeit kann dazwischen jede Menge Datenmanipulation erfolgen.

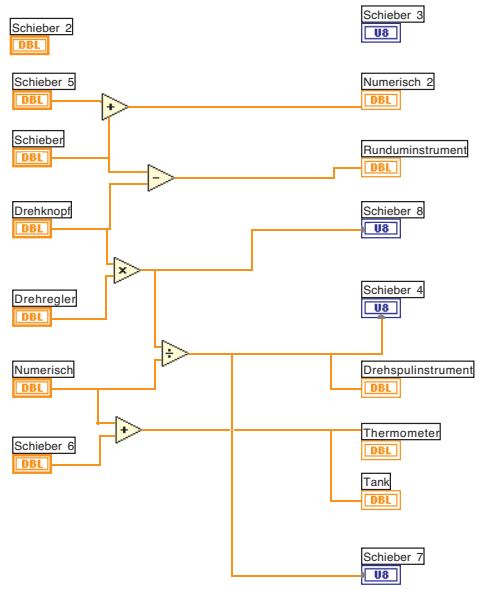
Man kann die Eingabegrößen mathematisch mit den Ausgabewerten verknüpfen und anzeigen lassen, kann aber auch Instrumente steuern, Daten in den Computer einlesen und mit LabVIEW nachbearbeiten und dann in ein File abspeichern, oder auch über das Internet verschicken. Die Möglichkeiten von LabVIEW sind in der Zwischenzeit schon weit über das Steuern von Messungen hinausgewachsen.

Die bereits beim Kauf von LabVIEW vorgefertigten Virtual Instruments (VIs) für die Kommunikation mit externen Geräten sind sehr hilfreich bei der Programmierung. Zum einen kann man sich bei den Demoprogrammen gute Tipps für die Umsetzung eigener Ideen holen, und zum anderen sind sie oft eine Ausgangsbasis für die Verwirklichung eines eigenen virtuellen Messinstrumentes. Seit es LabVIEW gibt, ist die langwierige Erstellung von Benutzeroberflächen im Laborbereich Geschichte. LabVIEW bietet die Möglichkeit, selbständig in kurzer Zeit qualitativ hochwertige Programme zu schreiben, die die Steuerung, die Datenerfassung und die Auswertung und Weiterverarbeitung voll automatisiert übernehmen. Für die meisten gängigen kommerziellen Geräte gibt es mittlerweile VIs.

Für alle, die dem graphischen Programmieren doch nicht ganz vertrauen, bietet LabVIEW auch die Möglichkeit, die alten vertrauten C-Routinen einzubinden und nur die neue Benutzeroberfläche mit LabVIEW zu erstellen. Dadurch hat man die Möglichkeit, alte, gut bewährte Programme mit den Vorteilen von LabVIEW zu verbinden und verwenden.



a)



b)

Abbildung 1:
a) Einige Ein- und Ausgabeinstrumente für die Erstellung eines virtuellen Instrumentes.
b) Mathematische Verknüpfung dieser Ein und Ausgabegeräte im Diagramm.

Im so genannten „Diagramm“ werden dann die einzelnen virtuellen Eingabeinstrumente mit den Ausgabeinstrumenten verknüpft. Dies geschieht auch auf einer graphischen Benutzeroberfläche. Alle auf dem Frontpanel platzierten „Controls“ und „Indicators“ scheinen als Symbol in der Programmieroberfläche (Diagramm) auf. Dort kann man dann wie in einem elektronischen Schaltplan die Eingabeinstrumente mit verschiedenen Operationen verknüpfen und dann das Endergebnis an den „Indicator“ ausgeben. Ein einfaches Beispiel ist in Abbildung 1b auf der rechten Seite zu sehen.

Eine weitere Stärke von LabVIEW ist nun, dass es die Möglichkeit bietet, mit der Hardware und dem Betriebssystem zu kommunizieren. Das Einlesen von Analogsignalen mit unterschiedlicher Abtastrate sowie das Ausgeben von Analogsignalen, die aus einem File ausgelesen werden, oder auch im Programm direkt errechnet werden können, zählt genauso wie das Ansteuern von Geräten über einen IEEE Bus zu den fundamentalen Bedienelementen von LabVIEW.

LabVIEW im Laserlabor des Instituts für Allgemeine Physik

Datenerfassung

Wir verwenden LabVIEW nun schon seit mehr als 10 Jahren, um verschiedene Laser, Spektrometer, Boxcar Analysatoren, Oszilloskope, Camac Interfaces, Analog-Digital Converter und Schrittmotoren zu steuern und Messdaten zu erfassen.

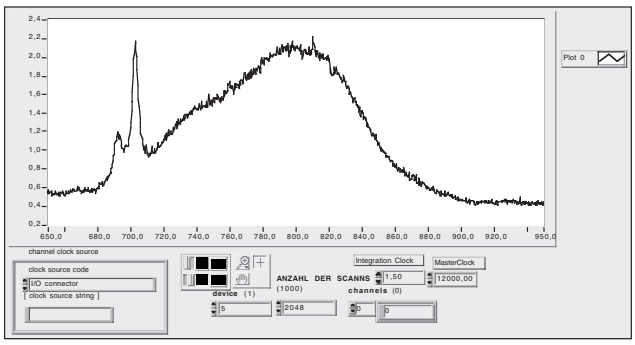


Abbildung 2: Das Frontpanel eines virtuellen Spektrometers.

In Abbildung 2 ist das selbstentwickelte VI eines bei uns im Labor verwendeten optischen Spektrometers dargestellt. Das Spektrum wird von einem CCD-Array Spektrometer aufgenommen und dann als Analogsignal an eine im Handel erhältliche multifunktionale AD-Wandlerkarte mit Timingfunktion geschickt. Mit LabVIEW wird dann das Auslesen des Spektrums und das Timing für das Spektrometer verwirklicht. Weiters besteht dann die Möglichkeit, das Spektrum weiterzuverarbeiten, zu analysieren und abzuspeichern. Dieses Spektrum dient zur permanenten Überwachung des Spektrums der Laserstrahlung eines Ti:Saphir Femtosekundenlasers [1, 2].

Weiters verwenden wir LabVIEW, um Massenspektren und Energieverteilungen von emittierten Sekundärteilchen zu messen [3]. Im Speziellen beschäftigen wir uns mit der grundlegenden Frage, wie das Laserlicht mit Materie wechselwirkt. Dazu verwenden wir ein Ultra-Kurzzeit Lasersystem mit einer Wellenlänge von 800nm und einer Pulsdauer von 30fs, sowie einen Excimerlaser mit einer ArF Füllung [4-6], der Laserstrahlung im UV-Bereich liefert. Diese beiden Laser werden je nach Art des Experiments zum Ionisieren von Teilchen bzw. zur Ablation von Materialien (Metalle, Halbleiter, biologisches Gewebe) verwendet. Die Steuerung und das Timing der Lasersysteme erfolgt mittels LabVIEW und der dazugehörigen Elektronik. Die Abbildung 3 zeigt schematisch die Steuerung des Messelektronik durch den Computer. Weiters wurde die Entwicklung einer Hornhautdrehbank (Eximer Laser Corneal Shaping ELCS [4, 7]) mittels LabVIEW-Steuerung durchgeführt.

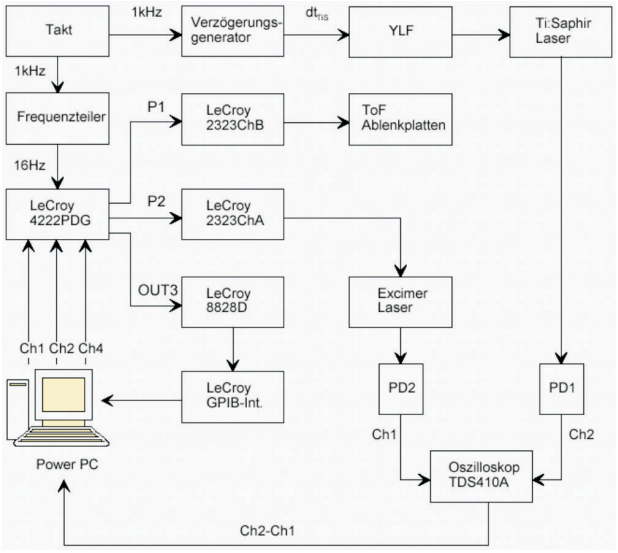


Abbildung 3: Schema der Steuerung der Laser, des Spektrometers und der Datenerfassung mit Hilfe des Computers. Mit Hilfe der beiden Photodioden PD1 und PD2 wurde die zeitliche Verzögerung des Excimerlaser relativ zum Ti:Saphir Laser gemessen.

Über programmierbare Verzögerungsgeneratoren (LeCroy 4222PDG und LeCroy 2323) wurde das Timing der beiden Laser (Neutralteilchendetektion bei der Laserablation) bzw. des Primärionenstrahls und des Lasers für die Nachionisation (Neutralteilchendetektion bei der Zerstäubung) eingestellt und mit dem Oszilloskop gemessen. Die Steuerung der beiden verwendeten Laser und das Auslesen des Messsignals vom Oszilloskop konnte mithilfe geeigneter Hardware von einem mit LabVIEW selbstentwickelten Programm mit Benutzeroberfläche gesteuert werden.

In weiteren LabVIEW-Programmen werden dann die Messsignale in Energieverteilungen umgerechnet mit Modellen verglichen.

Ein wichtiger Bestandteil des eben beschriebenen Experiments ist die Erfassung der Massenspektren von gesputterten Teilchen. Das dazu verwendete Spektrometer ist ein Flugzeitmassenspektrometer. Die Auswertung der

Flugzeitspektren und das Umrechnen der Flugzeitspektren in Massenspektren wird wieder von einem LabVIEW-Programm ausgeführt. Das Frontpanel des hierfür verwendeten Programms ist in Abbildung 4 zu sehen.

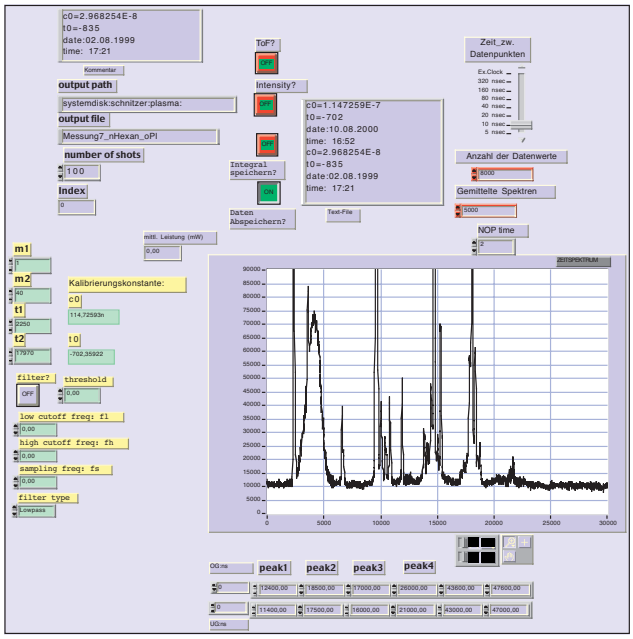


Abbildung 4: Teil der Benutzeroberfläche eines Programms zur Aufnahme von Flugzeitspektren von laser-nachionisierten Atomen und Molekülen.

Datenauswertung und Simulation

Neben der Hauptverwendung von LabVIEW als Datenerfassungs- und Gerätesteuerungsumgebung wird LabVIEW auch an Stelle von traditionellen Programmiersprachen oft vorteilhaft als Datenauswertungsumgebung eingesetzt. Durch die graphische Oberfläche, aber besonders wegen seiner vielzähligen Routinen zur Umwandlung von Datenformaten hat sich LabVIEW besonders dann als praktisch erwiesen, wenn es notwendig ist, verschieden abgespeicherte Daten weiterzuverarbeiten. Die graphische Oberfläche eignet sich auch gut für einfachere Simulationen, da praktisch alle notwendigen Funktionen (Integrierer, Summierer etc.) vorhanden sind und wie in einer Schaltung „verdrahtet“ werden können.

Updates

Die aktuelle Version von LabVIEW ist Version 6. Wir haben bisher im Wesentlichen mit allen Versionen bis einschließlich 4 gearbeitet. Die Umstellung auf neue Versionen ist meist problematisch, wenn man die doch recht komplexen Programme und immer wieder auftauchende Inkompatibilitäten beim Wechseln auf eine neue Version bedenkt. Im Prinzip sind die Programme aufwärts kompatibel, jedoch kommt es immer wieder vor, dass gewisse Funktionen in neueren Versionen nicht mehr unterstützt werden oder zumindest leicht geändert wurden. Eine Umstellung einer laufenden Messanordnung ist daher immer ein gewisses Risiko.

Bedingt verbessert wurde ein Manko von älteren LabVIEW Versionen, nämlich die nicht vorhandene Abwärtskompatibilität (Kompatibilität der VIs mit älteren Versionen). Man kann VIs aus der Version 6 im Format LabVIEW 5, aber nicht älteren Versionen abspeichern. VIs, die mit älteren Versionen geschrieben wurden, sind mit den oben erwähnten Einschränkungen mit LabVIEW 6 weiterzuverwenden, allerdings ist es nicht mehr möglich, VIs, die mit LabVIEW 6 bearbeitet wurden, in LabVIEW 4 oder älter zu verwenden.

Die Hilfe zu den einzelnen VIs gibt es seit Version 6 auch in Deutsch, was vielleicht für den einen oder anderen ganz angenehm ist, allerdings haben sich zu den deutschen Beschreibungen auch manche englische Beschreibungen dazugesellt. Die Suchroutinen in der LabVIEW 6 Hilfe sind einigermaßen übersichtlich gestaltet und lassen sich auch leicht bedienen.

Das große Plus, das sofort ins Auge sticht, ist die Tatsache, dass sich im Aufbau der Benutzeroberfläche zu den früheren Versionen nur wenig geändert hat. Es sind zwar eine ganze Reihe praktischer VIs dazugekommen, aber an den bisher gewohnten Möglichkeiten hat sich nicht viel geändert. So ist es kein großes Problem, mit der neuen verbesserten Version von LabVIEW zu arbeiten.

Literatur

[1] F. Krausz, „From femtochemistry to attophysics“, *Physics World*, **14**, 9 pp. 41-46, 2001 Sep

[2] T. Brabec and F. Krausz, „Intense few-cycle laser fields: Frontiers of nonlinear optics“, *Reviews of Modern Physics*, **72**, 2 pp. 545-591, 2000 Apr

[3] W. Husinsky and G. Betz, „Fundamental aspects of SNMS for Thin Film Characterization – experimental studies and computer simulations [Review]“, *Thin Solid Films*, **272**, 2 pp. 289-309, 1996

[4] V. Schmidt, W. Husinsky, R. Graf, F. Fitzal and M. Grabenwöger, "„Tissue perforation of vessel substitutes using a femtosecond Ti:Sapphire laser system“, *to be published in SPIE series*, pp., 2000

[5] A. Cortona, W. Husinsky and G. Betz, „Influence of adsorbates, crystal structure, and target temperature on the sputtering yield and kinetic-energy distribution of excited Ni atoms“, *Physical Review B-Condensed Matter*, **59**, 23 pp. 15495-15505, 1999

[6] M. Grabenwoger, F. Fitzal, J. Sider, C. Cseko, H. Bergmeister, H. Schima, W. Husinsky, P. Bock and E. Wolner, „Endothelialization of biosynthetic vascular prostheses after laser perforation“, *Ann Thorac Surg*, **66**, 6 Suppl pp. S110-4, 1998

[7] J. Altmann, G. Grabner, W. Husinsky, S. Mitterer, I. Baumgartner, F. Skorpik and T. Asenbauer, „Corneal Lathing Using the Excimer Laser and a Computer-Controlled Positioning System: Part I-Lathing of Epikeratoplasty Lenticules“, *Journal of Refr. and Corneal Surgery*, **7**, pp. 377-384, 1991

Personelle Veränderungen

Seit Anfang Juni 2001 arbeitet Herr **Werner Steinmann** (steinmann@zid.tuwien.ac.at, Nst. 42036) wieder halbtags in der Betreuung des Softwaredistributionsservers, anstelle von Frau Dipl.-Ing. Elisabeth Donnaberger, die Anfang Juni den ZID verlassen hat.

Ab 1. Oktober 2001 übernimmt Frau **Natalie Vejnoska** (vejnoska@zid.tuwien.ac.at, Nst. 42034) in der Abt. Standardsoftware die Nachfolge von Herrn Dipl.-Ing. Markus Klug im Software Setup.

Herr **Dipl.-Ing. Markus Klug** arbeitete von Mai 1998 bis Oktober 2000 und im August 2001 im Bereich des Campus Software Setup, mit Schwerpunkt bei den Aufbereitungsarbeiten von Microsoft-Produkten und UNIX-Anwendungen. Er war ein fleißiger, genauer und anerkannter Fachmann und Kollege. Wir wünschen ihm weiterhin viel Erfolg.

Herr **Gerold Mosinzer** (mosinzer@zid.tuwien.ac.at, Nst: 42023) arbeitet seit Anfang November halbtags als Unterstützung im Bereich Infrastruktur der Abt. Standardsoftware.

Herr **Michael Hofbauer** (hofbauer@zid.tuwien.ac.at, Nst. 42085) ist seit Anfang Juni im Bereich der Internet-Services für Studierende, Hardware-Support, tätig.

Herr **Manfred Hautzinger** (hautzinger@zid.tuwien.ac.at, Nst. 42087) unterstützt seit Anfang Juli die Abteilung Zentrale Services in der Unix-Systembetreuung (IBM SP).

Herr **Andreas Schulz** hat auf eigenen Wunsch den ZID verlassen. Er war etwa ein Jahr halbtags in der Abt. Zentrale Services tätig.

Seit Mitte September 2001 ist Herr **Anil Datta** (datta@zid.tuwien.ac.at, Nst. 42042) in der Abteilung Kommunikation im Referat Server tätig. Er wird primär Herrn DI Klasek im Bereich der Betreuung des Mail- und White Pages Services unterstützen.

Wir wünschen allen neuen Mitarbeiterinnen und Mitarbeitern viel Erfolg und Freude bei ihrer Tätigkeit am ZID.

ZID Beirat

Zur Unterstützung der notwendigen Kommunikation zwischen den Fakuläten und dem ZID wurde ein beratendes Gremium für IT-Angelegenheiten eingerichtet (ZID Beirat). Es besteht aus zwei vom Senat entsandten Mitgliedern und je einem Mitglied aus den einzelnen Fakultäten, das vom Dekan entsandt wird. Aus dem Senat wird je ein Mitglied aus dem Kreis der Studierenden und eines aus der Fakultät für Technische Naturwissenschaften und Informatik entsandt. Dieses Gremium wird mindestens viermal im Jahr vom Vorsitzenden des Beirates einberufen.

(siehe Betriebs- und Benutzungsordnung des Zentralen Informatikdienstes, § 10 (1))

Die Mitglieder des ZID Beirats sind:

Univ. Prof. Karlheinz Schwarz	Vorsitz	Senat	kschwarz@theochem.tuwien.ac.at
Andreas Traxler		Senat	atrax@fsmat.htu.tuwien.ac.at
DI Christian Schranz		BI	sc@fest.tuwien.ac.at
Ao.Prof. Erasmus Langer		ET	erasmus.langer@tuwien.ac.at
Univ.Prof. Georg Franck-Oberaspach		RA	franck@osiris.iemar.tuwien.ac.at
Ao. Prof. Helmut Böhm	Stv.	MB	hjb@ilfb.tuwien.ac.at
Dr. Robert Sablatnig		TNI	sab@prip.tuwien.ac.at

Wählleitungen

01 / 589 32	**Normaltarif**
07189 15893	**Online-Tarif** (50 km um Wien)

Datenformate:
300 - 56000 Bit/s (V.92) MNP5/V.42bis/V.44
PPP
ISDN Synchronous PPP

Auskünfte, Störungsmeldungen

Sekretariat
Tel.: 58801-42001
E-Mail: sekretariat@zid.tuwien.ac.at

TUNET

Störungen
Tel.: 58801-42003
E-Mail: trouble@noc.tuwien.ac.at

Rechneranmeldung
E-Mail: hostmaster@noc.tuwien.ac.at

Telekom
Hotline: 08 (nur innerhalb der TU)
E-Mail: telekom@noc.tuwien.ac.at
Chipkarten, Abrechnung: 58801-42008

IT-Sicherheit
E-Mail: security@tuwien.ac.at

Service-Line Abt. Standardsoftware
Tel.: 58801-42004
E-Mail: sekretariat@sts.tuwien.ac.at

Systemunterstützung
Computer Help Line 42124
E-Mail: pss@zid.tuwien.ac.at
Web: sts.tuwien.ac.at/pss/

Campussoftware
E-Mail: campus@zid.tuwien.ac.at
gd@zid.tuwien.ac.at

Zentrale Server, Operating
Tel.: 58801-42005
E-Mail: operator@zid.tuwien.ac.at

Internet-Räume
Tel.: 58801-42006
E-Mail: studhelp@zid.tuwien.ac.at

Öffnungszeiten

Sekretariat

Freihaus, 2. Stock, gelber Bereich

Montag bis Freitag, 8 Uhr bis 13 Uhr

- Ausgabe und Entgegennahme von Formularen für Benutzungsbewilligungen für Rechner des ZID,
- Internet-Service für Studierende: Vergabe von Benutzungsbewilligungen, die nicht automatisch erteilt werden können,
- allgemeine Beantwortung von Benutzeranfragen, Weiterleitung an fachkundige Mitarbeiter.

Telefonische Anfragen: 58801-42001

Operator-Ausgabe

Freihaus, 2. Stock, roter Bereich
Montag bis Freitag, 7 Uhr 30 bis 20 Uhr

- Ausgabe für Farbdrucker.
- Passwortvergabe für das Internet-Service für Studierende.
- Ausgabe diverser Informationen für Studierende, Weiterleitung von Anfragen an fachkundige Mitarbeiter.

Internet-Räume

Die Internet-Räume (in den Gebäuden Karlsplatz, Freihaus, Gußhausstraße, Treitlstraße, Gumpendorferstraße, Bibliothek, Favoritenstraße) sind im Regelfall entsprechend den Öffnungszeiten des jeweiligen Gebäudes geöffnet. An Sonn- und Feiertagen ist kein Betrieb. Siehe auch `http://student.tuwien.ac.at/internetraeume/`
Tutoren (Studienassistenten) sind in den Internet-Räumen im Freihaus und in der Favoritenstraße anwesend (Zeiten unter: `http://student.tuwien.ac.at/tutoren/`).

Personalverzeichnis

Telefonliste, E-Mail-Adressen

Zentraler Informatikdienst (ZID)
der Technischen Universität Wien
Wiedner Hauptstraße 8-10 / E020
A - 1040 Wien
Tel.: (01) 58801-42000 (Leitung)
Tel.: (01) 58801-42001 (Sekretariat)
Fax: (01) 58801-42099
Web: www.zid.tuwien.ac.at

Leiter des Zentralen Informatikdienstes:

W. Kleinert	42010	kleinert@zid.tuwien.ac.at

Administration:

A. Müller	42015	mueller@zid.tuwien.ac.at
M. Grebhann-Haas	42018	grebhann-haas@zid.tuwien.ac.at

Öffentlichkeitsarbeit

I. Husinsky	42014	husinsky@zid.tuwien.ac.at

IT-Sicherheit

U. Linauer	42026	linauer@zid.tuwien.ac.at

Abteilung Zentrale Services

www.zid.tuwien.ac.at/zserv/

Leitung

P. Berger	42070	berger@zid.tuwien.ac.at
W. Altfahrt	42072	altfahrt@zid.tuwien.ac.at
J. Beiglböck	42071	beiglboeck@zid.tuwien.ac.at
P. Deinlein	42074	deinlein@zid.tuwien.ac.at
P. Egler	42094	egler@zid.tuwien.ac.at
H. Eigenberger	42075	eigenberger@zid.tuwien.ac.at
C. Felber	42083	felber@zid.tuwien.ac.at
H. Flamm	42092	flamm@zid.tuwien.ac.at
W. Haider	42078	haider@zid.tuwien.ac.at
E. Haunschmid	42080	haunschmid@zid.tuwien.ac.at
M. Hautzinger	42087	hautzinger@zid.tuwien.ac.at
M. Hofbauer	42085	hofbauer@zid.tuwien.ac.at
P. Kolmann	42095	kolmann@zid.tuwien.ac.at
F. Mayer	42082	fmayer@zid.tuwien.ac.at
J. Pfennig	42076	pfennig@zid.tuwien.ac.at
M. Rathmayer	42086	rathmayer@zid.tuwien.ac.at
M. Roth	42091	roth@zid.tuwien.ac.at
J. Sadovsky	42073	sadovsky@zid.tuwien.ac.at
E. Srubar	42084	srubar@zid.tuwien.ac.at
Werner Weiss	42077	weisswer@zid.tuwien.ac.at

Abteilung Kommunikation

nic.tuwien.ac.at

Leitung

J. Demel	42040	demel@zid.tuwien.ac.at
S. Beer	42061	beer@zid.tuwien.ac.at
F. Blöser	42041	bloeser@zid.tuwien.ac.at
G. Bruckner	42046	bruckner@zid.tuwien.ac.at
S. Dangel	42066	dangel@zid.tuwien.ac.at
A. Datta	42042	datta@zid.tuwien.ac.at
T. Eigner	42052	eigner@zid.tuwien.ac.at
S. Geringer	42065	geringer@zid.tuwien.ac.at
J. Haider	42043	jhaider@zid.tuwien.ac.at
M. Hanold	42062	hanold@zid.tuwien.ac.at
P. Hasler	42044	hasler@zid.tuwien.ac.at
S. Helmlinger	42063	helmlinger@zid.tuwien.ac.at
H. Kainrath	42045	kainrath@zid.tuwien.ac.at
J. Klasek	42049	klasek@zid.tuwien.ac.at
W. Koch	42053	koch@zid.tuwien.ac.at
T. Linneweh	42055	linneweh@zid.tuwien.ac.at
I. Macsek	42047	macsek@zid.tuwien.ac.at
F. Matasovic	42048	matasovic@zid.tuwien.ac.at
W. Meyer	42050	meyer@zid.tuwien.ac.at
R. Vojta	42054	vojta@zid.tuwien.ac.at
Walter Weiss	42051	weiss@zid.tuwien.ac.at

Abteilung Standardsoftware

sts.tuwien.ac.at

Leitung

A. Blauensteiner	42020	blauensteiner@zid.tuwien.ac.at
C. Beisteiner	42021	beisteiner@zid.tuwien.ac.at
J. Donatowicz	42028	donatowicz@zid.tuwien.ac.at
G. Gollmann	42022	gollmann@zid.tuwien.ac.at
M. Holzinger	42025	holzinger@zid.tuwien.ac.at
A. Klauda	42024	klauda@zid.tuwien.ac.at
H. Mastal	42079	mastal@zid.tuwien.ac.at
H. Mayer	42027	mayer@zid.tuwien.ac.at
G. Mosinzer	42023	mosinzer@zid.tuwien.ac.at
E. Schörg	42029	schoerg@zid.tuwien.ac.at
R. Sedlaczek	42030	sedlaczek@zid.tuwien.ac.at
W. Selos	42031	selos@zid.tuwien.ac.at
B. Simon	42032	simon@zid.tuwien.ac.at
A. Sprinzl	42033	sprinzl@zid.tuwien.ac.at
W. Steinmann	42036	steinmann@zid.tuwien.ac.at
P. Torzicky	42035	torzicky@zid.tuwien.ac.at
N. Vejnoska	42034	vejnoska@zid.tuwien.ac.at