

infoforum

Zentrum für Informationsverarbeitung der Universität Münster
Jahrgang 29, Nr. 3 – Dezember 2005 ISSN 0931-4008

Inhalt

Editorial.....	2
ZIV-Aktuell	3
CERT der Uni Münster hilft Urheberrechtsverletzungen zu vermeiden.....	3
Direkter Anschluss des Hochschulstandorts Münster an das X-WiN.....	4
Modem/ISDN-Einwahldienste ab 1.1.2006: „www@home“!.....	5
Juristische Heimarbeiter.....	6
Neue VPN-Technologie an der Universität.....	8
perMail goes Unicode.....	9
Neues von MATLAB.....	10
Neuerungen bei Beschaffung und Lizenzierung von SPSS-Produkten.....	11
Handbücher des RRZN Hannover.....	13
ZIV-Präsentation	14
Seitennavigation unter Imperia.....	14
Erfahrungsbericht: XP als Hauptbenutzer.....	14
ZIVGrid – Grid-Computing mit Condor.....	19
ZIV-Lehre	21
ZIV-Lehre wird geschätzt.....	21
Veranstaltungen in der vorlesungsfreien Zeit (Frühjahr 2006).....	21
Kommentare zu den Veranstaltungen.....	22
ZIV-Regularia	25
Fingerprints.....	25



Impressum

inform
ISSN 0931-4008

Westfälische Wilhelms-Universität
Zentrum für Informationsverarbeitung (Universitätsrechenzentrum)
Röntgenstr. 9-13
48149 Münster

E-Mail: ziv@uni-muenster.de
WWW: <http://www.uni-muenster.de/ZIV/>
Redaktion: E. Sturm (☎ 83-31679, ✉ sturm@uni-muenster.de)
Satz: K. Hovestadt
Satzsystem: StarOffice 7
Druck: Drucktechnische Zentralstelle

Auflage dieser Ausgabe: 1400

Editorial

St. Ost



Das Schneechaos, das vor einigen Tagen den Norden des Münsterlandes lahmlegte, ist auch am ZIV nicht ohne Spuren vorübergegangen. Gegen 3.30 Uhr am Samstag Morgen wurde ich durch die Notmeldung geweckt, die Klimaanlage in der Einsteinstraße täte es nicht. Nun sind zu hohe Temperaturen für Server in der Tat gefährlich: Sie funktionieren nicht mehr und neigen zu Hardware-Defekten. So musste schnell etwas geschehen. Sich anziehen und den PKW freikratzen war kein Problem, nur kam ich mit meinen Sommerreifen einfach nicht durch den 30 cm hohen Neuschnee. Ein ebenfalls alarmierter winterbereifter Kollege hatte mehr Glück und kam zur Einsteinstraße durch. Dort verhinderten Schneeverwehungen, dass sich die Eingangstür öffnen ließ. Zusammen mit dem ebenfalls eingetroffenen technischen Dienst der Universität konnte man dann aber das ZIV betreten. Ausgefallen war die Klimaanlage, die den Raum mit den Rechnernetzkomponenten kühlen sollte. Dort war es inzwischen 40°C warm. Glücklicherweise sind Netzkomponenten wärme härter als Server; ausgefallen ist nichts (außer der Klimaanlage). Paradoxerweise haben Klimaanlagen mit frostiger Außenluft größere Problem als mit sommerlicher Wärme.

Was kann man daraus lernen? Selbst wenn Notfallpläne funktionieren, braucht man bei extremen Situationen ein bisschen Glück, in unserem Fall in Form von Winterreifen, um mit Problemen fertig zu werden.

ZIV-Aktuell

CERT der Uni Münster hilft Urheberrechtsverletzungen zu vermeiden

Thorsten Küfer

Das WWU-CERT sieht sich einer steigenden Zahl von Urheberrechtsverletzungen konfrontiert.

Das Computer Emergency Response Team (CERT) der Universität Münster (1) ist Anlaufstelle für Missbrauchs-, Angriffs- und Beschwerdefälle unterschiedlichster Art bzgl. der Universitätsrechner. Zu den Tätigkeiten gehört u. a. die Begrenzung von Virusinfektionen, das Stoppen von Spamversand sowie die Bearbeitung von Beschwerden über Urheberrechtsverletzungen. Letztere machen dabei einen schnell wachsenden Anteil aus.

Mit Einführung des Digital Millennium Copyright Act (DMCA) (2) von 1998 wurde die Verfolgung von Urheberrechts-Delikten in den USA vereinfacht und Internetprovider (ISPs) können für die Taten ihrer Nutzer mitverantwortlich gemacht werden. Im September 2003 ist auch in Deutschland nach Vorgabe der EU-Richtlinie „Urheberrecht in der Informationsgesellschaft“ das Urheberrechtsgesetz (3) novelliert worden, so dass das Herunterladen von rechtswidrig hergestellten Kopien, also von solchen, für die der Anbieter kein Verwertungs- bzw. Vervielfältigungsrecht hat (wie Musik oder Filme aus Tauschbörsen), bestraft werden kann.

„Wer Musik oder Filme unberechtigt im Internet zum Download anbietet, muss auf jeden Fall mit einer Geldstrafe rechnen. Das kann teuer werden. Hinzu kommen noch die zivilrechtlichen Schadensersatzforderungen der Rechte-Inhaber. Diese bemessen sich primär an der Menge der angebotenen Werke. Wer also Tausende von Files unerlaubt zum Download bereit hält, muss im schlimmsten Falle mit Kosten im fünf- oder sechsstelligen Bereich rechnen.“ (4)

Um Urheberrechtsdelikte aufzuspüren, haben die Rechte-Inhaber spezielle Firmen (wie z. B. (5)) beauftragt, die alle Tauschbörsen, Newsgruppen, Webseiten, IRC usw. automatisch nach Material durchsuchen und entsprechend dem DMCA Beschwerden (engl. „Copyright Infringement Notices“) an die verantwortlichen Provider verschicken.

Die Internetprovider in Deutschland sind gegenüber den Rechte-Inhabern nicht dazu verpflichtet diesen mitzuteilen, welcher Nutzer hinter einer IP-Adresse steckt, unter der Urheberrechtsverletzungen im Internet begangen worden sind. Die Herausgabe von personenbezogenen Daten kann im Allgemeinen nur auf richterlichen Beschluss erfolgen. Die Universität Münster als ISP für alle Mitarbeiter und Studenten muss allerdings auf Beschwerden der Rechte-Inhaber in angemessener Form reagieren und Urheberrechtsverletzungen seitens seiner Nutzer abstellen, um nicht zu Schadensersatz verpflichtet zu werden. Da Urheberrechtsverletzungen ein Verstoß gegen §3(3)7 der Nutzungsordnung (6) sind, können die verantwortlichen Nutzer vorübergehend oder dauerhaft von der Nutzung der DV-Dienste der Universität Münster ausgeschlossen und zu Kostenersatz herangezogen werden.

Ein weiterer für die Universität relevanter Aspekt des neuen Urheberrechts ist die Verwendung von Texten oder Bildern aus fremden Quellen auf den WWW-Seiten. Bevor diese in eine Webseite eingebaut werden dürfen, ist das Einverständnis des Rechte-Inhabers einzuholen. Beim Einbau in die Webseite sind die Quelle anzugeben und mit dem Einverständnis verbundene Auflagen genau zu befolgen. Dies alles sollte bei der Veröffentlichung von Webseiten unbedingt beachtet werden, um die Universität vor Abmahnungen und den damit verbundenen Kosten zu schützen.

Weiterführende Informationen zur rechtlichen Lage bei der Behandlung von Urheberrechtsverletzungen und Kommentare zu aktuellen Gerichtsurteilen und deren Auswirkung auf Hochschulen gibt es auf den Seiten des DFN Vereins (7).

(1) WWU-CERT <cert@uni-muenster.de>

(2) DMCA <<http://www.copyright.gov/legislation/dmca.pdf>>

- (3) Urheberrechtsgesetz
<<http://www.bundesjustizministerium.de/media/archive/126.pdf>>
- (4) Das neue Urheberrecht <<http://www.kopien-brauchen-originale.de/>>
- (5) BayTSP, Inc. <<http://www.baytsp.com/>>
- (6) Benutzungsordnung des ZIV <<http://www.uni-muenster.de/ZIV/Organisation/Benutzungsordnung.html>>
- (7) Forschungsstelle Recht des DFN <<http://www.dfn.de/content/beratung/rechtimdfn/archiv0/>>

Direkter Anschluss des Hochschulstandorts Münster an das X-WiN

M. Speer

Das Deutsche Forschungsnetz, an das die meisten Hochschulen und Forschungseinrichtungen in Deutschland angeschlossen sind, wird derzeit auf eine neue technologische Plattform, das sog. „X-WiN“, gestellt. Dabei wird Münster anders als bei der Vorgängertechnologie, dem G-WiN, ein eigener X-WiN-Backbone-Standort.

Durch den in Räumen der Universität angesiedelten X-WiN-Gerätstandort ergibt sich die Möglichkeit des direkten Anschlusses der Universität Münster an das X-WiN. Der X-WiN-Standort Münster selber wird zur Erhöhung der Verfügbarkeit doppelt an das X-WiN angebunden werden. Diese doppelte Anbindung führt auf vollständig unterschiedlichen Wegen zu zwei anderen X-WiN-Standorten (vgl. Abb. 1, Quelle: DFN-Verein). Derzeit (Stand Dezember 2005) befindet sich der Standort noch im Aufbau.



Abb. 1: X-WiN Topologie (breit: Faser, schmal: gemietete Wellenlängen)
Stand Nov. 2005

Diese direkte Anschlussmöglichkeit an das X-WiN bedeutet eine hohe Flexibilität in Bezug auf die Anlusstechnik und Bandbreite für die Universität und die im sog. Cluster mitversorgten Einrichtungen: Universitätsklinikum und Fachhochschule (vgl. Abb. 2). Die vertraglich vereinbarte Bandbreite des X-WiN-Anchlusses beträgt 600 Mbps. Damit ist die Universität Münster gut gerüstet, um auch in Zukunft die steigenden Datenmengen neuer multimedialer Anwendungen (z.B. Videokonferenzen) zuverlässig zu bewältigen.

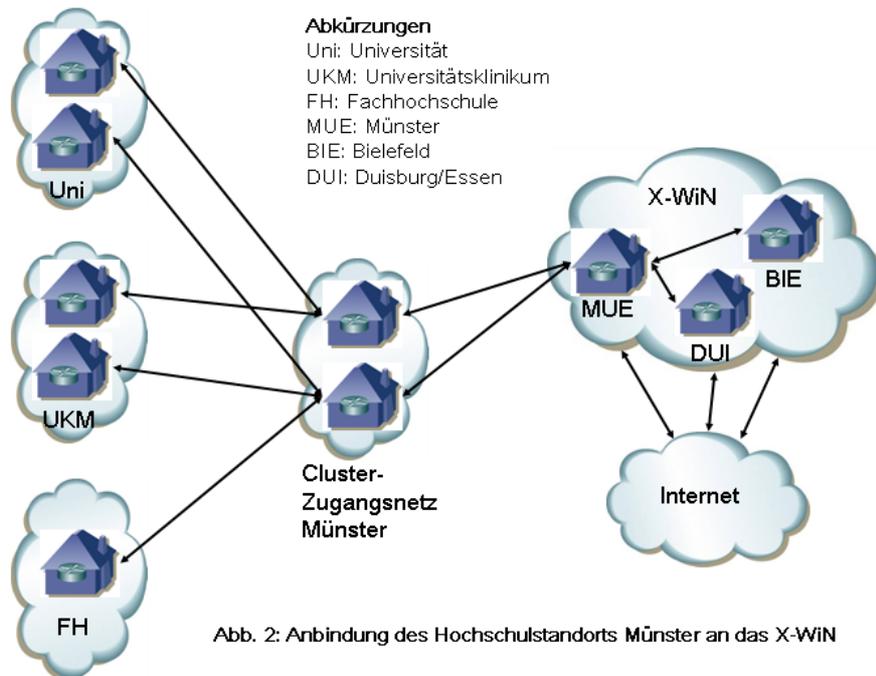


Abb. 2: Anbindung des Hochschulstandorts Münster an das X-WiN

Modem/ISDN-Einwahldienste ab 1.1.2006: „wwu@home“!

M. Speer

Die verschiedenen vom ZIV in Zusammenarbeit mit der Fernsprechzentrale bereitgestellten Einwahldienste für den Modem/ISDN-Zugang zum Universitätsnetz und zum Internet werden auch zukünftig in bewährter Form weiterbetrieben. Die Verfügbarkeit bzw. Kapazität einiger Dienste wurde sogar verbessert. Der Artikel gibt einen Überblick über die aktuelle Situation.

Folgende Einwahlrufnummern / Einwahldienste stehen zur Verfügung:

- 0193-604: „wwu@home“ (nur für Telekom-Telefonanschlüsse)

Von vielen Telekom-Telefonanschlüssen in Münster und Umgebung aus kann die äußerst günstige „wwu@home“-Einwahlmöglichkeit genutzt werden. Kunden der Citykom Münster können dieses Angebot leider nicht nutzen. Die Details der Nutzungsvoraussetzungen findet man auf der „wwu@home“-Homepage: www.uni-muenster.de/ZIV/wwuhome. An dieser Stelle sei nur die attraktive Tarifstruktur (ab 0,77 Cent/Min. rund um die Uhr, 40 Cent monatliche Grundgebühr) genannt.

Dieser bisher in Kooperation mit der Deutschen Telekom unter dem Namen „uni@home plus“ betriebene Einwahldienst wird nun vom ZIV und der Fernsprechzentrale eigenständig in einer aus Nutzersicht unveränderten Form weiterbetrieben. Die Verfügbarkeit dieses Dienstes wird demnächst durch die Hinzunahme weiterer Region-50-Bereiche (für 1,29 Cent/Min.) sogar noch erweitert.

- 0997: „Teleport“

Dieses zusammen mit der Deutschen Telekom realisierte Einwahlangebot kommt für Anschlüsse in Wohnheimen des Studentenwerks Münster in Frage. Genutzt werden kann das Angebot nur von Teleport-Vertragskunden. Nähere Auskünfte über die Tarife für die normale Telefonie und für die Einwahl in das Universitätsnetz/Internet erfährt man über das Studentenwerk bzw. Teleport.

In diesem Jahr wurde die Zahl der verfügbaren Teleport-Einwahlschlüsse schrittweise von 600 auf 750 erhöht.

- 0251 / 83-60666: „Allgemeiner Zugang“

Dieses Angebot kann weltweit vom Telefonanschluss eines beliebigen Telefonanbieters (Deutsche Telekom, Citykom Münster, ...) aus benutzt werden. Es ist auch keinerlei zusätzliche Registrierung, Anmeldung o. ä. erforderlich. Für die Nutzung reichen eine gewöhnliche ZIV-Benutzerkennung und ein Netzzugangspasswort aus (<https://user.uni-muenster.de/exec/nutzer>). Als Einwahlkosten fallen die „normalen“ Telefongebühren des Telefonanbieters an. Zu beachten ist aber insbesondere für XXL-

Tarifikunden der Deutschen Telekom, dass diese XXL-Tarifierung keinen Vorteil bei Online-Diensten sicherstellt (siehe www.t-com.de/tel/blacklist-xxl), auch nicht für diese neue Rufnummer. Aus dem universitätsinternen Telefonnetz kann diese Rufnummer auch direkt kostenlos angewählt werden: 60666.

Dieser Zugang löst die zukünftig wegfallenden Rufnummern 0251 / 880 7750 („Uni@home“) und 0251 / 83-66 („universitätsintern“) ab. Nutzer dieser beiden Nummern sollten unbedingt ab sofort auf die 0251 / 83-60666 umstellen.

Juristische Heimarbeiter

U. Weber-Steinhaus

Die IVV 3 der Rechtswissenschaftlichen Fakultät entwickelt ein innovatives Konzept für den campusweiten bzw. häuslichen Zugriff auf die juris-Datenbank. Das Konzept lässt sich auf andere Literaturdatenbanken an der Universität übertragen.

Juristische Literaturrecherche verlagert sich immer mehr vom Papier hin zur elektronisch abrufbaren Information.¹

Die Rechtswissenschaftliche Fakultät bietet dementsprechend ein umfassendes juristisches online-Angebot. Neben verschiedenen juristischen CD-ROMs und fakultätseigenen Angeboten finden sich auf der Webseite der Fakultät LexisNexis, beck-online, westlaw und juris als bedeutsame Datenbankanbieter juristischer online-Informationen.² Ein Blick auf die Recherche-Website der Rechtswissenschaftlichen Fakultät ist also allemal lohnenswert.

Insbesondere juris stellt nicht nur für die rechtswissenschaftliche Forschung, sondern auch für andere Mitglieder der Universität, die bei ihrer Arbeit auf Rechtsinformationen angewiesen sind, ein umfassendes Angebot an Rechtsprechung, Literatur und Normen bereit. Aus diesem Grund hat sich die Rechtswissenschaftliche Fakultät anlässlich der Neuauflage des juris-Vertrages dafür eingesetzt, dass dieses in der Bundesrepublik größte juristische Informationsangebot nicht wie bisher nur auf Fakultätsebene verfügbar ist, sondern im Rahmen einer Campuslizenz nunmehr allen Universitätsangehörigen zur Verfügung steht.

Da Juristen bekanntlich rund um die Uhr arbeiten, wollen sie diese Dienste auch vom häuslichen Arbeitsplatz aus nutzen. Der LexisNexis-Verlag, mit dem die Fakultät eine Kooperationsvereinbarung unterhält, ermöglicht diesen häuslichen Zugriff auf ihre rechtlichen Datenbankinhalte sowohl für Wissenschaftler als auch für Studierende unter Verwendung eines VPN-Zugangs. Anders gelagert sind jedoch die lizenzrechtlichen Regelungen von beck-online und juris, die zwar einen campusweiten Zugriff für alle Studierenden, nicht aber den häuslichen Zugriff erlauben. Der Heimarbeitsplatz bleibt hier dem Wissenschaftler vorbehalten.

Diese restriktive Lizenzpolitik beruht bei juris u. a. darauf, dass etwaigem Missbrauch vorgebeugt werden soll. Insbesondere soll verhindert werden, dass Anwälte über einen Universitätszugang den Informationsdienst nutzen, ohne ihrerseits für die erheblichen Kosten aufzukommen.

Mit diesem rechtlichen Lizenzkonzept konfrontiert, stellte sich für die IVV 3 der Rechtswissenschaftlichen Fakultät die Frage, wie dieses wohl technisch umgesetzt werden könne. Auf der einen Seite galt es den campusweiten Zugriff für alle Universitätsangehörigen zu realisieren, andererseits beim häuslichen Zugriff nutzerspezifisch zwischen Wissenschaftlern und Studierenden zu differenzieren.

Fakultätszugriff

Da der Umgang mit juris für Wissenschaftler und Studierende der Rechtswissenschaftlichen Fakultät zum täglichen Arbeitswerkzeug gehört, ist ein möglichst unkomplizierter Zugriff innerhalb der Fakultät unabdingbar. Der Zugriff innerhalb der Rechtswissenschaftlichen Fakultät ist daher über einen IP-Bereich geregelt, so dass der juristische

¹ Vgl. nur Noak, Die großen Fünf: Professionelle Online-Dienste für Juristen im Test, http://www.jura.uni-duesseldorf.de/informationsrecht/materialien/studie_onlinedienste.pdf.

² Vgl.: <http://www.jura.uni-muenster.de/go/forschen/recherche.html>.

Informationsbedarf direkt via Webbrowser abgedeckt werden kann. Diese Art des Zugangs stellt keine Herausforderung dar und wird seit langem erfolgreich praktiziert.

Der wissenschaftliche Heimarbeitsplatz

Problematischer ist hingegen der nutzerspezifische Heimarbeitsplatz. Hier helfen Restriktionen auf Basis von IP-Bereichen nicht weiter. Vielmehr ist dies ein Problem des Identitätsmanagements, welches es unabhängig etwaiger zukünftiger Gesamtlösungen vorab dringend zu lösen galt. Mit Hilfe neu erworbener VPN-Hardware von Cisco, die Dank des ZIV trotz Probebetriebes schon für dieses Projekt zur Verfügung steht (siehe auch den folgenden Artikel), kann nunmehr ein nutzerspezifischer VPN-Zugang geschaltet werden. Der Nutzer benötigt hierfür die entsprechende Clientsoftware mit einem speziellen juris-Profil, welches vom ZIV entwickelt wurde und von der Webseite der IVV 3 der Rechtswissenschaftlichen Fakultät heruntergeladen werden kann. Voraussetzung ist, dass der Nutzer sich in der Gruppe u0vpn hat eintragen lassen. Berechtigt sind alle Wissenschaftler und Angehörige der Verwaltung.³ Das Problem des Zugangs für Wissenschaftler am heimischen Arbeitsplatz ist damit gelöst.

Campusweiter Zugriff

Das für den Heimarbeitsplatz entwickelte Konzept, das auf jedem Rechner die Installation eines Cisco-VPN-Clients erfordert, ist für die flächendeckende Versorgung der Universität mit juris-Zugängen nicht erstrebenswert. Die IVV 3 der Rechtswissenschaftlichen Fakultät hat sich daher nach anderweitigen Möglichkeiten des Zugangs umgesehen.

Für den campusweiten Zugriff liegt die Lösung in der Verwendung eines Terminalservers (`jurarecherche.uni-muenster.de`), der quasi als „Application Gateway“ die Verbindung zu juris herstellt. Windows-Server 2003 als Betriebssystem stellt gleichzeitig sicher, dass die Rechercheergebnisse vom Nutzer auf seinem lokalen Drucker ausgegeben werden können; die Verwendung von teuren Citrix-Clients ist damit obsolet. Da diesem Server die alleinige Aufgabe obliegt, eine Verbindung zu dem juris-System herzustellen (geplant ist auch die Einbindung von beck-online), wäre die Verwendung eines echten Servers eine Ressourcenvergeudung. Der Server wurde daher mittels VM-Ware virtualisiert und so konfiguriert und beschränkt, dass allein eine Verbindung zu juris via Webbrowser hergestellt werden kann. Zudem kann auf diesen Server nur von solchen Rechnern zugegriffen werden, deren Namen in eine Positivliste der IVV 3 der Rechtswissenschaftlichen Fakultät aufgenommen worden sind, womit Terminalserver-hopping und andere lokale Einwahlmöglichkeiten ausgeschlossen sind. Diese Liste wird auf Antrag berechtigter Personen (IVV-Leiter) erweitert. Die Antragsteller müssen dafür Sorge tragen und zusichern, dass auf die betreffenden Rechner kein Zugriff von außerhalb der Universität von nichtberechtigten Nutzern stattfinden kann.

Da das ZIV sich ausdrücklich vorbehält, IP-Adressen ohne weiteres zu ändern, sind DNS-Namen und keine IP-Adressen im Rahmen der Beantragung zu verwenden. Es obliegt den Antragstellern, die beantragten Bereiche bei Bedarf nachzupflegen und die IVV 3 der Rechtswissenschaftlichen Fakultät über etwaige Änderungen zu informieren.

Des Weiteren ist von den Antragstellern sicherzustellen, dass von den berechtigten Rechnern auch nur Universitätsangehörige den Terminalserver anwählen können, d. h. Gastkennungen erhalten keinen Zugang. Das notwendige Formular findet sich ebenfalls auf der oben angegebenen Website. Erste Bereiche der Universität wie Verwaltung und Universitätsbibliothek sind bereits auf diese Weise mit juris versorgt.

Die IVV 3 der Rechtswissenschaftlichen Fakultät hat damit einen Beitrag zum praktischen Einsatz von Identitätsmanagement geleistet, welches als Beispiel für ähnliche differenzierte Datenbankzugänge innerhalb der Universität dienen kann.

(Akad. Dir. Dr. U. Weber-Steinhaus ist Leiter der IVV 3 der Rechtswissenschaftlichen Fakultät der Universität Münster.)

³ Vgl. zu den weiteren Formalitäten unter <http://www.jura.uni-muenster.de/go/forschen/recherche/juris.html>.

Neue VPN-Technologie an der Universität

A. Forsmann

VPN (Virtual Private Network) ist ein Verfahren, um Dienste eines Netzwerks von außerhalb nutzen zu können.

Die bisherige VPN-Technologie an der Universität, basierend auf dem Point-to-Point-Tunnelprotocol (PPTP), ist durch eine IPSec-basierende VPN-Technologie ergänzt worden. IPSec (IP Security) ist eine Erweiterung des Internetprotokolls (IP), um Vertraulichkeit, Authentizität und Integrität der Datenkommunikation zu ermöglichen. IPSec ermöglicht eine sichere Kommunikation über ungesicherte Netzwerke, wie z. B. das Internet, indem u. a. die Daten mit dem 3DES-Verfahren verschlüsselt werden können. 3DES ist eine Weiterentwicklung des Data Encryption Standard (DES) und ist ein sehr sicheres Verfahren um Daten zu verschlüsseln.

Mit der neu beschafften VPN-Hardware lässt sich der VPN-Dienst virtualisieren, d. h. mehrere verschiedene VPN-Gateways können mit einer einzigen Hardware definiert werden. Damit ist es möglich, Sicherheitsanforderungen unterschiedlicher Netzwerkbereiche (z. B. verschiedener Fachbereiche) gerecht zu werden. Neben einem allgemeinen VPN-Gateway für die Universität ist das ZIV so in der Lage, in Abstimmung mit den IV-Versorgungseinheiten, Fachbereichen oder Instituten für diese eigene VPN-Gateways bereitzustellen.

Nach dem Aufbau einer VPN-Verbindung z. B. zu einem VPN-Gateway eines Fachbereichs befindet sich dann der Rechner im Netzwerk des Fachbereichs. Somit können berechnete Nutzer auch von außerhalb Dienste eines internen Netzwerkes des Fachbereichs nutzen, die sonst aus Sicherheitsgründen (oder anderen Gründen) über das Internet nicht unmittelbar zur Verfügung stehen.

Für den Aufbau einer VPN-Verbindung muss der Nutzer den kostenlosen VPN-Client der Firma Cisco installiert haben. Die Installation und Benutzung des Cisco-VPN-Clients ist sehr nutzerfreundlich. Für alle gängigen Betriebssysteme (Windows, Linux, Mac OS) stehen den Angehörigen der Universität und des UKM die Cisco-VPN-Clients auf den Webseiten des ZIV zum Download zur Verfügung.

Neben der Installation des VPN-Clients muss noch – abhängig davon, zu welchem VPN-Gateway eine Verbindung aufgebaut werden soll – ein bestimmtes VPN-Profil in den Client importiert werden. Für das allgemeine VPN-Gateway der Universität muss z. B. das Profil „vpnstandard.uni-muenster.de“ importiert werden. Im Cisco-VPN-Client können auch mehrere VPN-Profile gleichzeitig hinterlegt werden (siehe Abbildung 1).

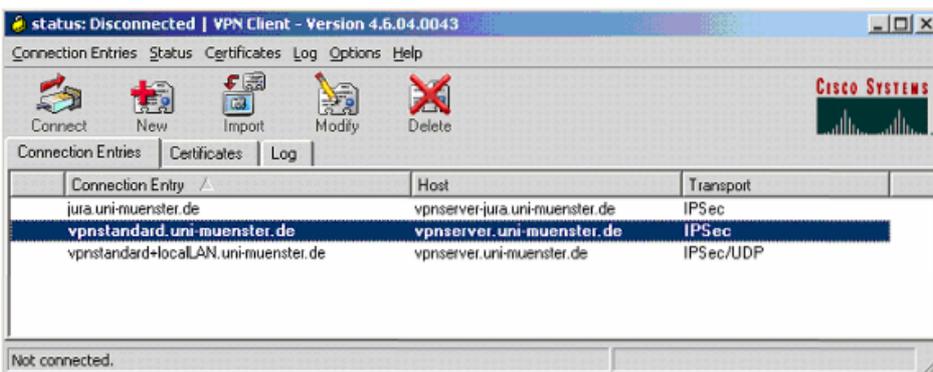


Abbildung 1. Screenshot eines Cisco VPN-Client mit mehreren importierten VPN-Profilen.

Wie bei dem bisherigen PPTP-basierenden VPN muss sich der Nutzer für das allgemeine VPN-Gateway der Universität mit seiner ZIV-Kennung und seinem Netzzugangspasswort authentifizieren. Möchte der Nutzer sich aber in ein bestimmtes VPN-Gateway eines Fachbereichs einwählen, muss er sich als `user@xyz` mit seinem Netzzugangspasswort einloggen, wobei `xyz` für den Namen des entsprechenden VPN-Gateways steht. Ob ein

Nutzer die Berechtigung hat, sich in ein bestimmtes VPN-Gateway einzuwählen, hängt davon ab, ob der Nutzer in einem zum VPN-Gateway gehörigen Projekt und damit einer bestimmten Nutzergruppe zugeordnet ist. Diese Nutzergruppen können online unter:

<https://user.uni-muenster.de/exec/wwuben/wwuben.php>

von den zuständigen Projektleitern verwaltet werden; so können die Projektleiter Nutzer, die einen ZIV-Account haben, dem Projekt und somit auch der Nutzergruppe selbstständig online hinzufügen oder aber auch entfernen.

Der Aufbau eines VPN-Tunnels aus einem Heimnetzwerk mit einem DSL-Anschluss (oder ISDN bzw. analogen Anschluss) stellt sich mit der neuen VPN-Variante erheblich einfacher da als vorher, da die VPN-Verbindung auch über die NAT-Funktion (Network Address Translation) der Router (z. B. des DSL-Routers) problemlos funktioniert. Bei der bisherigen PPTP-basierenden VPN-Lösung war dies ein häufig auftretendes Problem, da viele Routertypen NAT für das PPTP-Protokoll nicht unterstützten.

Erste Pilotprojekte mit dieser neuen VPN-Technologie wurden bereits durchgeführt (siehe z. B. den vorstehenden Artikel „Juristische Heimarbeiter“).

In Kürze wird der Regelbetrieb aufgenommen werden. Alles weitere zu diesem Thema finden Sie dann unter:

<http://www.uni-muenster.de/ziv/vpn>

Alle diejenigen, die nicht so lange warten möchten, können aber auch jetzt schon diese VPN-Technologie im Zusammenhang mit dem VPN-Standardzugang testen. Auf folgender Seite können Cisco-VPN-Clients, VPN-Profilen und Installationsanleitungen zzt. heruntergeladen werden:

<http://zivkiosk.uni-muenster.de/cisco-vpn>

perMail goes Unicode

R. Perske

Voraussichtlich zum Jahreswechsel wird die Version 2.0 unserer Webmail-Software *perMail* in Betrieb gehen.

Wer die Entwicklung von perMail im ablaufenden Jahr verfolgt hat, dem wird auf <https://permail.uni-muenster.de/help-de-changes.html> immer wieder der Punkt „Vorbereitende Arbeiten für zukünftige Erweiterungen“ aufgefallen sein. Diese Erweiterungen lassen sich mit einem Begriff zusammenfassen: Unicode.

Unicode bezeichnet das weltweit einheitliche Kodierungssystem, in dem jedes Zeichen jeder Sprache unabhängig von Spracheinstellungen, Software, Betriebssystem und deren Herstellern eine eindeutige Code-Nummer erhält, welche von allen Unicode-fähigen Datenverarbeitungssystemen gleich verstanden wird (siehe <http://www.unicode.org>). Durch die Vielfalt älterer Kodierungssysteme konnte es geschehen, dass ein Brite £35 eintippt und der Betrag in Amerika als \$35 angezeigt wird; dieser Fauxpas kann mit Unicode nicht mehr passieren.

Selbst wenn Sie von Unicode noch nie etwas gehört haben, haben Sie es wahrscheinlich schon längst verwendet: Aktuelle Windows-Systeme arbeiten intern konsequent mit Unicode, das gleiche gilt für immer mehr Linux-Distributionen, Office-Produkte, WWW- und E-Mail-Programme. Allerdings begegnet man überall noch älterer Software, die noch nicht Unicode-tauglich ist, daher wird leider gerade in E-Mails Unicode noch viel zu selten verwendet.

Auch perMail 1 beherrscht seit Jahren die Darstellung von Unicode und die Umwandlung zahlreicher älterer Zeichenkodierungen nach Unicode. Kürzlich wurden noch einige ISO-2022-Kodierungen ergänzt, so dass jetzt neben üblichen E-Mails mit verschiedenen lateinischen (wie in Łódź), griechischen (Ελληνικά), kyrillischen (Русский), hebräischen (תּיבּרית) oder chinesischen (中文) Schriften auch übliche koreanische (한국어) und japanische (日本語) E-Mails trotz älterer Kodierung richtig dargestellt werden können. Bei der Einstellung Textsatz=Bild gilt das sogar dann, wenn Ihr Rechner gar nicht über entsprechende Zeichensätze verfügt.

Was perMail 1 aufgrund früherer Beschränkungen bei HTML-Formularen jedoch noch nicht anbietet, ist das Schreiben von E-Mails mit solchen Schriftzeichen: Ausschließlich Zeichen aus dem westeuropäischen Zeichensatz „ISO 8859-1 Latin 1“ können bei der Erstellung von E-Mails verwendet werden. Nicht einmal das Euro-Zeichen (€) gehört zu diesem Zeichensatz; es konnte daher beim Schreiben von E-Mails mit perMail bisher nicht verwendet werden.

Eine Universität mit ihrem weltweiten Kommunikationsbedarf sollte natürlich universellere Möglichkeiten bieten. Daher habe ich bereits vor anderthalb Jahren mit der Umwandlung von perMail 1 in perMail 2 begonnen und sehr viel Freizeit in dieses Projekt investiert. Äußerlich unterscheiden sich beide Versionen nur geringfügig, im Inneren wurde jedoch die komplette Zeichenkettenverarbeitung von ISO 8859-1 (8-Bit-Zeichenkodierung) auf Unicode (32-Bit-Zeichenkodierung UCS-4 und 8-Bit-Transportkodierung UTF-8) umgestellt. Da E-Mail-Verarbeitung nur wenig mehr als eine sehr komplexe Zeichenkettenverarbeitung darstellt, wurde praktisch das komplette Programm umgeschrieben.

Zahlreiche der dabei nötigen Verbesserungen und Neuentwicklungen sind in den letzten Monaten auch in perMail 1 eingeflossen und werden daher schon intensiv von Ihnen genutzt. Nur in zwei Punkten bleibt die Unicode-Unterstützung in perMail 2 zumindest anfangs leider unvollständig: *Reguläre Ausdrücke* in den Wegsortierregeln bleiben auf ISO-8859-1 beschränkt; und die positionssabhängigen Buchstabenformen im Arabischen und in einigen anderen Schriften werden zumindest bei `Textsatz=Bild` noch nicht beachtet.

perMail 2 wird also alle Schriftzeichen in Ihre E-Mails einbauen, die Sie in Ihrem WWW-Programm eintippen können. Uns Europäer interessiert dabei natürlich vor allem das Euro-Zeichen. Um jetzt auch mit einer deutschen Tastatur koreanische oder griechische Schriftzeichen eintippen können, benötigen Sie auf Ihrem Rechner eine entsprechende Software. In aktuellen Betriebssystemen ist solche Software bereits enthalten und muss von Ihnen nur aktiviert werden; suchen Sie dazu bitte in Ihren Hilfeseiten nach *IME (Input Method Editor)*, nach *Eingabegebietsschema* und/oder nach *Tastatur-layout*. Für einzelne fremde Schriftzeichen reicht sicherlich auch die *Zeichentabelle*.

Wenn Sie perMail 2 bereits ausprobieren möchten, können Sie gerne am Testbetrieb teilnehmen: Unter <https://permail2.uni-muenster.de> finden Sie die Loginseite. Melden Sie entdeckte Fehler und Unstimmigkeiten bitte an perske@uni-muenster.de.

Teilnehmer am Testbetrieb sollten bitte kurzzeitige Betriebsunterbrechungen nicht als Fehler ansehen und beachten, dass Konfigurations-Textdateien (Fußzeilen, Textbausteine, Wegsortierregeln usw.) von perMail 2 im UTF-8-Format statt wie bisher im ISO-8859-1-Format abgelegt werden. Wenn Sie diese Dateien mit perMail 2 modifizieren und sie anschließend wieder mit perMail 1 verwenden, dann werden Umlaute und einige Sonderzeichen falsch dargestellt bzw. ausgewertet.

Die sonstigen in perMail 1 eingeflossenen Änderungen des ablaufenden Jahres betreffen meist nur Kleinigkeiten: Die Funktion *Text ausrichten* zur Formatierung einer neuen E-Mail wurde verbessert. Nach dem PGP/MIME-Standard signierte und verschlüsselte E-Mails können jetzt verifiziert bzw. entschlüsselt und weiter verarbeitet werden. Die Verschlüsselungsroutinen wurden an GnuPG 1.4 angepasst. Fehlende PGP-Schlüssel werden automatisch vom Schlüsselservers des DFN nachgeladen. Die Bedienoberfläche kann bereits auf der Loginseite ausgewählt werden. Beim Löschen hinterlegter Dateien wurde eine Sicherheitsabfrage eingebaut. Die *Zentrale Nutzerverwaltung Online* unter <https://user.uni-muenster.de/exec/nutzer> bietet die Möglichkeit, ohne erneute Passworteingabe perMail zu nutzen; auch für die Zusammenarbeit mit kommenden Single-Signon- und Portal-Systemen ist perMail jetzt gerüstet.

Selbstverständlich bleibt die Entwicklung nicht bei perMail 2.0 stehen: Eine ganze Reihe sinnvoller Vorschläge aus dem Nutzerkreis, deren Realisierung ich aus Zeitgründen zurückstellen musste, wartet bereits.

Neues von MATLAB

B. Süselbeck

Im jetzt zu Ende gehenden Jahr wurde die zentrale Matlab-Lizenz erneut erweitert

Die zentrale Lizenz für Matlab konnte auch im Jahr 2005 vom ZIV im Zusammenarbeit mit mehreren Fachbereichen erweitert werden. Sie umfasst zur Zeit folgende Produkte (Anzahl der Lizenzen in Klammern):

- Matlab (40)
- Simulink (40)
- Compiler (2)
- Database Toolbox (10)
- Fuzzy Logic Toolbox (10)
- Genetic Algorithm & Direct Search Toolbox (10)
- Image Acquisition Toolbox (10, nur für Windows)
- Image Processing Toolbox (10)
- Mapping Toolbox (10)
- Neural Network Toolbox (10)
- Optimization Toolbox (10)
- Partial Differential Equation Toolbox (10)
- Signal Processing Toolbox (10)
- Symbolic Toolbox (10)
- Statistics Toolbox (10)
- Wavelet Toolbox (10)

Nähere Auskünfte erteilt: Dr. B. Süselbeck (☎31686, suselbe@uni-muenster.de)

Neuerungen bei Beschaffung und Lizenzierung von SPSS-Produkten

Chr. Schild

Seit Dezember 2005 läuft die neue Lizenzperiode für SPSS-Produkte. Mit SPSS Version 13 und dem vom ZIV angebotenen Lizenzserver kann ab sofort SPSS kostenlos im Universitätsnetz benutzt werden.

Die Hochschulen des Landes NRW haben seit vielen Jahren einen Landeslizenzvertrag mit SPSS abgeschlossen und können dadurch SPSS-Produkte zu günstigen Konditionen beziehen. Diese Vereinbarung gilt für die Nutzung durch Forschungseinrichtungen, aber insbesondere auch durch Mitarbeiter/innen und Studierende, sofern die Nutzung ausschließlich wissenschaftlichen Zwecken dient.

Für die neue Lizenzperiode vom 01. Dezember 2005 bis 31. November 2006 haben sich mit der neuen Softwareversion SPSS 13 einige wichtige Neuerungen ergeben. Mit SPSS 13 ist ein so genanntes „Concurrent License“-Modell, also eine Netzlizenz möglich. Hierbei wird nicht pro Installation eine Lizenz benötigt, vielmehr gibt es einen Lizenzserver, der zentral alle Lizenzen verwaltet. Bei Programmstart (die SPSS-Software wird weiterhin auf dem eigenen Rechner liegen) verbindet sich das System mit diesem Lizenzserver, holt sich eine freie Lizenz und gibt die Nutzung frei. Auf diese Weise kann die vorhandene Anzahl an Lizenzen von mehreren Anwendern gleichzeitig benutzt werden. Der Lizenzserver wird redundant ausgelegt, so dass Betriebsstörungen möglichst vermieden werden.

Da mit der Verwendung der Netzlizenzen über den Lizenzserver an der Anzahl der nötigen Lizenzen gespart und der Verwaltungsaufwand reduziert werden kann, hat sich das ZIV entschlossen, für diese Lizenzperiode den Lizenzserver für das Produkt SPSS 13 allen Einrichtungen und Nutzern der Universität als Dienst kostenlos anzubieten. In Zukunft reicht für Nutzer innerhalb des Universitätsnetzes also die Kenntnis des Lizenzservers aus, um SPSS 13 nutzen zu können. Eine Bestellung und Bezahlung jeder einzelnen SPSS13-Installation entfällt dann also.

Hierzu gibt es folgende Ausnahmen. Der Lizenzserver ist zunächst von Arbeitsplätzen innerhalb des Universitäts-Netzes erreichbar. Um SPSS aber auf Heimarbeitsplätzen oder Laptops nutzen zu können, muss man entweder bei Programmstart online gehen

und auch während der jeweiligen Nutzungszeit von SPSS online bleiben, da nur dann der Lizenzserver einsetzbar bleibt, oder man kann weiterhin Einzelplatzlizenzen verwenden. Diese Einzelplatzlizenzen sind nur in limitierter Anzahl vorhanden und müssen weiterhin käuflich im ZIV erworben werden. Hier gilt der alte Preis von 50 Euro. Dieser Preis gilt auch für den Einsatz der alten Version 12, die nicht unter dem Lizenzserver einsetzbar ist.

Wir empfehlen daher, möglichst schnell auf die neue Version 13 aufzurüsten und den Lizenzserver zu nutzen.

Eine weitere wichtige lizenzrechtliche Neuerung mit der neuen Lizenzperiode ist: Sollten sie eine SPSS-Einzelplatz-Lizenz erwerben, so stehen Ihnen ab sofort zwei Autorisierungen zu, so dass Sie z. B die Anwendung gleichzeitig auf Ihrem System am Arbeitsplatz und einem Laptop installieren können.

Meistgenutztes Produkt des Lizenzvertrags ist das SPSS. Aktuell liegt es uns in der deutschen Version 13 (mit den Komponenten Base, Regression Models, Advanced Models, Tables, Trends, Categories, Exact Test, Missing Value Analysis, Conjoint und Custom Tables) vor.

Für folgende Produkte sind Lizenzen vorhanden:

- SPSS 13 deutsch
- SPSS 13 englisch
- SPSS 12.0.1 deutsch
- SPSS 12.0.1 englisch
- SPSS 11.5 deutsch
- SPSS 11.5 englisch
- SPSS 11.0.2 for Macintosh
- DATA ENTRY Builder 4.0
- AMOS 6.0 englisch
- AMOS 5.0 englisch
- Answer Tree 3.1 deutsch
- Answer Tree 3.1 englisch

Zu beachten ist, dass die Lizenz für die Windows-Versionen 11.5 letztmalig verlängert wurde. Wir empfehlen Nutzern der Version 11.5 dringend auf eine möglichst aktuelle Version aufzurüsten.

Weitere Details zu SPSS, zum Beispiel, wie sie die Software beziehen können, entnehmen sie bitte unseren Webseiten zu Verteilung von SPSS Software⁴.

Im Laufe des Lizenzjahres erwarten wir die Auslieferung einer SPSS-Version 14. Das ZIV hat eine Mailingliste⁵ für alle SPSS-Nutzer eingerichtet, auf der Fragen, Termine, Tipps&Tricks usw. diskutiert werden können. Insbesondere werden dort auch alle Neuerungen zu SPSS angekündigt.

SPSS-Verteilung: <http://www.uni-muenster.de/ZIV/Software/SoftwareVerteilungSPSS.html>

SPSS-Mailingliste: <http://listserv.uni-muenster.de/mailman/listinfo/spss-1>

⁴ [SPSS-Verteilung: http://www.uni-muenster.de/ZIV/Software/SoftwareVerteilungSPSS.html](http://www.uni-muenster.de/ZIV/Software/SoftwareVerteilungSPSS.html)

⁵ [SPSS-Mailingliste: http://listserv.uni-muenster.de/mailman/listinfo/spss-1](http://listserv.uni-muenster.de/mailman/listinfo/spss-1)

Handbücher des RRZN Hannover

W. Kaspar

Das Zentrum für Informationsverarbeitung der Universität Münster bietet eine Auswahl der Handbücher des Regionalen Rechenzentrums für Niedersachsen (RRZN) der Universität Hannover zum preiswerten Erwerb durch Studierende und Bedienstete der Universität an. Wenden Sie sich bitte unter Vorlage einer Immatrikulations- bzw. einer Dienstbescheinigung an unseren Broschürenverkauf (Einsteinstraße 60, Obergeschoss, Zimmer 104, montags bis freitags von 9.00 bis 12.00 Uhr).

Folgende Titel sind zzt. verfügbar:

- Acrobat 5.0, PDF-Dateien erstellen und publizieren (135 Seiten) 1. Auflage
- Java 2, Grundlagen und Einführung (410 Seiten) 2. Auflage
- Java Script (220 Seiten) 4. Auflage
- Outlook 2003 (184 Seiten) 2. Auflage
- Perl, Eine Einführung (280 Seiten) 1. Auflage
- Photoshop CS - Einführung (208 Seiten) 1. Auflage
- PHP 5, Fortgeschrittene Techniken (224 Seiten) 1. Auflage
- PHP, Grundlagen - Erstellung dynamischer Webseiten (198 Seiten) 2. Auflage
- Publizieren im World Wide Web (280 Seiten) 4. Auflage
- SPSS - Grundlagen (156 Seiten) 9. Auflage
- SPSS für Fortgeschrittene (240 Seiten) 5. Auflage
- Staroffice & Open Office (158 Seiten) 1. Auflage
- Visual Basic 6.0 - Grundlagen (172 Seiten) 9. Auflage
- Windows Server 2003, Aufbau und Verwaltung eines Netzwerkes (240 Seiten) 2. Auflage
- Windows Server 2003, Netzwerkadministration (180 Seiten) 2. Auflage
- Windows XP, Grundlagen für Anwender (198 Seiten) 1. Auflage
- Word 2003, Grundlagen (202 Seiten) 1. Auflage
- Word 2002, Fortgeschrittene Anwendungen (188 Seiten) 7. Auflage

Die Auswahl der vom Zentrum für Informationsverarbeitung angebotenen Titel richtet sich nach der Nachfrage durch Benutzer und der Verfügbarkeit beim RRZN.

Es wird gebeten, von Anfragen an das RRZN bezüglich der Handbücher abzusehen. Das RRZN hat mit Herausgabe und Vertrieb der Handbücher genug zu tun und sollte deshalb sowenig wie möglich durch zusätzliche Nachfragen belastet werden. Sie können sich aber gern Inhaltsverzeichnisse aller Handbücher sowie Leseproben und Übungsdateien im WWW ansehen. Alle Anfragen wegen Verfügbarkeit, Preis usw. der Handbücher richten Sie bitte an unseren Broschürenverkauf.

Die vom RRZN angebotenen Handbücher dürfen nur in Einzelstücken an Studierende und Bedienstete zum Selbstkostenpreis abgegeben werden. Sie sind ausschließlich zu deren persönlichem Gebrauch bestimmt.

Noch eine Bemerkung zum Schluss: Die günstigen Abgabebedingungen der RRZN-Handbücher basieren auf dem Kooperationsprinzip des „eine Hand wäscht die andere“. Sind Sie ggf. bereit, Neuerscheinungen der Handbücher unter fachlichen und didaktischen Gesichtspunkten Korrektur zu lesen? Das RRZN sucht Lektoren.

ZIV-Präsentation

Die Artikel dieser neuen Rubrik verkünden nicht etwas, das aktuell bekanntgemacht werden soll (wie bei ZIV-Aktuell), sondern präsentieren Informationen zu Soft- und Hardware oder auch zu Dienstleistungen, die für die Universität von Interesse sind.

Seitennavigation unter Imperia

A. Scheffer

Seit ihrer Einführung wurde die automatisch generierte Seitennavigation für Imperia stark erweitert. Inzwischen gibt es auch eine Dokumentation mit einführenden Beispielen für den Einsteiger und fortgeschrittene Imperia-Anwender.

Wie schon in vorhergehenden **inforum**-Artikeln (u. a. in Nr. 1/2005) beschrieben, wurde das Web-Content-Management-System Imperia durch diverse Zusatzmodule erweitert – unter anderem mit einem Programm zur automatischen Erzeugung von Navigationselementen auf jeder Webseite. Neben der Hauptnavigation, die zentral im Kopf einer jeden Seite positioniert ist, existieren Navigationsmöglichkeiten auf beiden Seiten eines damit maximal dreispaltigen Layouts. Während die rechte Seite für Verweise zu Seiten ausserhalb des eigenen Bereiches dient und somit wahlweise weggelassen werden kann, bedient die Navigationsstruktur auf der linken Seite die örtliche Subnavigation und ist damit eine notwendige Orientierungshilfe.

Obwohl nahezu vollautomatisch generiert, hat insbesondere diese Navigation aufgrund vieler Nutzerwünsche mit der Zeit an Konfigurierbarkeit und damit an Komplexität gewonnen. Man kann mittlerweile nicht nur die Reihenfolgen der Links beeinflussen, einige weglassen oder den angezeigten Navigationsbaum mit einer Einstiegstiefe versehen sondern zudem mit Leerzeilen, Überschriften, Kategorienamen und externen Links das Angezeigte weiter strukturieren und erweitern. Auf der einen Seite gibt diese Einstellvielfalt den Seitengestaltern ein mächtiges Werkzeug an die Hand, auf der anderen Seite wirft selbst eine vollständig vorkonfigurierte Navigation beim Einstieg in die Materie manchmal Fragen auf.

Seit kurzem gibt es jetzt eine Dokumentation mit einführenden Beispielen, die auf den Internetseiten des ZIV unter www.uni-muenster.de/ZIV/Content--CMS.html abrufbar ist. Sie bietet sowohl grundlegende Informationen für den Einsteiger als auch einen Überblick über die diversen Konfigurationsmöglichkeiten für den fortgeschrittenen Imperia-Anwender.

Erfahrungsbericht: XP als Hauptbenutzer

St. Ost

Dieser Artikel wendet sich an alle Windows-Nutzer, die es gewohnt sind, ständig mit Administrator-Rechten zu arbeiten.

Eines der größten Sicherheitsprobleme im Windows-Umfeld entspringt der Gewohnheit der meisten Nutzer, ständig mit Windows-Administrationsrechten zu arbeiten. Ein Windows-Administrator kann in seinem System tun und lassen, was er will. So verständlich dieser Wunsch ist, so groß ist der Schaden, wenn Administrationsrechte in die falschen Hände geraten. In der Regel besitzt ein Virus, der es trotz aller Schutzvorkehrungen ins System geschafft hat, die Rechte, die derjenige hat, der sich den Virus gefangen hat. Ist derjenige Administrator, so hat es der Virus leicht: Er kann die Spuren seiner Existenz und seines Tuns verstecken, beliebigen Schaden auf dem infizierten System anrichten, sensible Informationen des Nutzers ausspähen, usw.

Diese Gewohnheit hat historische Gründe. Windows unterschied lange Zeit nicht wirklich zwischen Administratoren und Nutzern. Erst Windows NT, dann Windows 2000 und Windows XP machten es möglich, relativ schmerzfrei ohne permanente Administrationsrechte zu arbeiten. Aber es wäre unfair, dieses alleine Microsoft anzulasten. Viele Windows-Entwickler haben es spät gelernt, sauber zwischen Nutzer- und Administrationsrechten zu trennen und ihre Software möglichst so zu schreiben, dass man besondere Rechte lediglich zur Installation benötigt.

Um es klar zu sagen: Es geht nicht darum, dem Nutzer die Administrations-Rechte für seinen Rechner zu nehmen. Es geht darum, diese Rechte nur dann zu haben, wenn man sie benötigt.

Technische Vorbemerkung

Windows besitzt ein umfangreiches System von Rechten, bestimmte Dinge auf dem Rechner tun zu dürfen. Handhabbar wird dieses System durch die Einführung von Gruppen. Eine Gruppe steht symbolhaft für eine typische Nutzungsweise des Rechners und ist mit bestimmten für die Nutzungsweise nötigen Rechten verbunden. Wird ein Nutzer Mitglied einer Gruppe, so hat er auch die Rechte dieser Gruppe. Es gibt vier Hauptgruppen:

Gast

Ein anonymer System-Nutzer. Seine Rechte sind die eines **Benutzers**. Die Universalität lehnt die anonyme Nutzung ihres Netzes ab. Diese Gruppe sollte auf ihrem System also leer sein und die zugehörige Nutzerkennung **Gast** sollte gesperrt sein.

Benutzer

Mitglieder der Benutzer-Gruppe haben nur Zugriff auf ihre eigenen Daten. Es ist ihnen nicht möglich, Systemverzeichnisse zu verändern. Anwendungen, die von Microsoft für Windows 2000 oder Windows XP zertifiziert wurden, laufen ordnungsgemäß mit Benutzerrechten und gefährden die System-Integrität nicht. **Benutzer** können Drucker nur dann einrichten, wenn die Druckertreiber bereits installiert sind.

Hauptbenutzer

Zusätzlich zur den Rechten der **Benutzer** haben **Hauptbenutzer** das Recht, Systembereiche insofern zu verändern, dass sie Programme nicht nur für sich selbst sondern auch für andere installieren können. Sie können andere systemweite Vorgänge durchführen, zum Beispiel das Ändern der Systemzeit oder das Erstellen von Benutzerkennungen und Freigaben. Hauptbenutzer können Druckertreiber nur dann installieren, wenn sie zusätzlich über das Recht *Laden und Entfernen von Gerätetreibern* verfügen. Der eigentliche Systembereich dagegen bleibt vor dem Hauptbenutzer geschützt.

Administratoren

Administratoren haben den vollen Zugriff auf alle Systemkomponenten und sind für die grundlegenden Arbeiten am System zuständig.

Es gibt weitere Gruppen für bestimmte Aufgaben. Notebook-Besitzer sind wahrscheinlich an der Gruppe **Netzwerkskonfigurations-Operatoren** interessiert, die insbesondere die WLAN-Konfiguration ermöglicht. Will man seinen Rechner von außen über den Remotedesktop nutzen, so muss man Mitglied der Gruppe **Remotedesktopbenutzer** sein.

Das Prinzip, Rechte über Gruppenmitgliedschaften zu verwalten, erleichtert vieles. Will man etwa wissen, *wer* auf einem Rechner *was* tun darf, so genügt es, sich die lokalen Gruppen anzusehen: Nur *wer* da eingetragen ist, der darf auch *was*.

Administrator auf Zeit

Klickt man mit der rechten Maustaste auf einen Programmnamen und hält dabei die Umschalttaste gedrückt, so öffnet sich ein Kontext-Menü, das den zusätzlichen Auswahlpunkt **Ausführen als ...** enthält. Wählt man diesen Punkt aus, so öffnet sich ein Fenster:



Nach Eingabe des lokalen Administrator-Passwortes wird das ursprünglich ausgewählte Programm gestartet. Dieses eine Programm hat, und kein anderes, für seine Laufzeit Administrationsrechte.

Freunden der Windows-Kommandozeile kann auch geholfen werden. Der Befehl `runas` führt einen bestimmten Befehl mit anderen Rechten aus. Zum Beispiel startet der Befehl `runas /profile /user:Administrator cmd.exe` eine zweite Kommandozeile, deren geänderte Rechte man dem Fensterrahmen ansieht.



Natürlich kann (und sollte) man andere Befehle mit dem `runas`-Kommando ausführen.

Grundinstallation

Man sollte nicht übertreiben: Die Grundinstallation erfolgt als Administrator. Gemeint sind folgende Tätigkeiten, die an dieser Stelle nur aufgeführt sind und die an anderer Stelle beschrieben werden müssen:

- Windows-Installation
- Netzkonfiguration mit DHCP
- Eintragen des Rechners in eine Active-Directory-Domäne
- Installation des EPO-Klienten zur Installation und Parametrisierung des McAfee-Virenschutzes
- Installation des SMS-Klienten zur einfachen Software-Installation
- Sich selbst, in meinem Fall den Nutzer ost@wwu, in die Gruppe der **Hauptbenutzer** eintragen.

Am Ende der Grundinstallation ist der Rechner in die DV-Infrastruktur der Universität eingebettet. Sein System wird regelmäßig gewartet. Der Virenschutz ist und bleibt aktuell.

Was geht ...

Was mich betrifft: Eigentlich geht fast alles. Einige Programme brauchen zur Installation Administrator-Rechte. Entweder bekommt man dies zu Anfang mitgeteilt oder die Installationsroutine blendet selbstständig das „Ausführen als“-Fenster ein. Installiert habe ich:

- Adobe Reader 7.0.5
- GNU Privacy Guard 1.4.2
- IrfanView 3.90
- JEdit 4.2
- Java SE Runtime 5.0 Update 5
- Microsoft ActiveSync 4.1
- Microsoft Office Professional 2003
- MikTex 2.4
- Mozilla Firefox 1.5
- Mozilla Thunderbird 1.0.7
- Nero 6
- Password Safe 2.13
- SSH Tectia Client 5.0
- Subversion 1.2.3
- VMware Workstation 5.0
- WinRAR 3.5.1

Natürlich ist ihre Software-Liste eine andere. Aber sie vermag Ihnen einen Eindruck vermitteln, was alles problemlos als Nicht-Administrator läuft.

„Nero“ benötigt normalerweise Administrator-Rechte zum Brennen von CDs oder DVDs. Der Hersteller stellt auf seiner Web-Seite ein kleines Dienstprogramm „Nero Burnright“ zur Verfügung, mit der es möglich ist, Brennrechte an Nicht-Administratoren zu vergeben.

... und was nicht geht

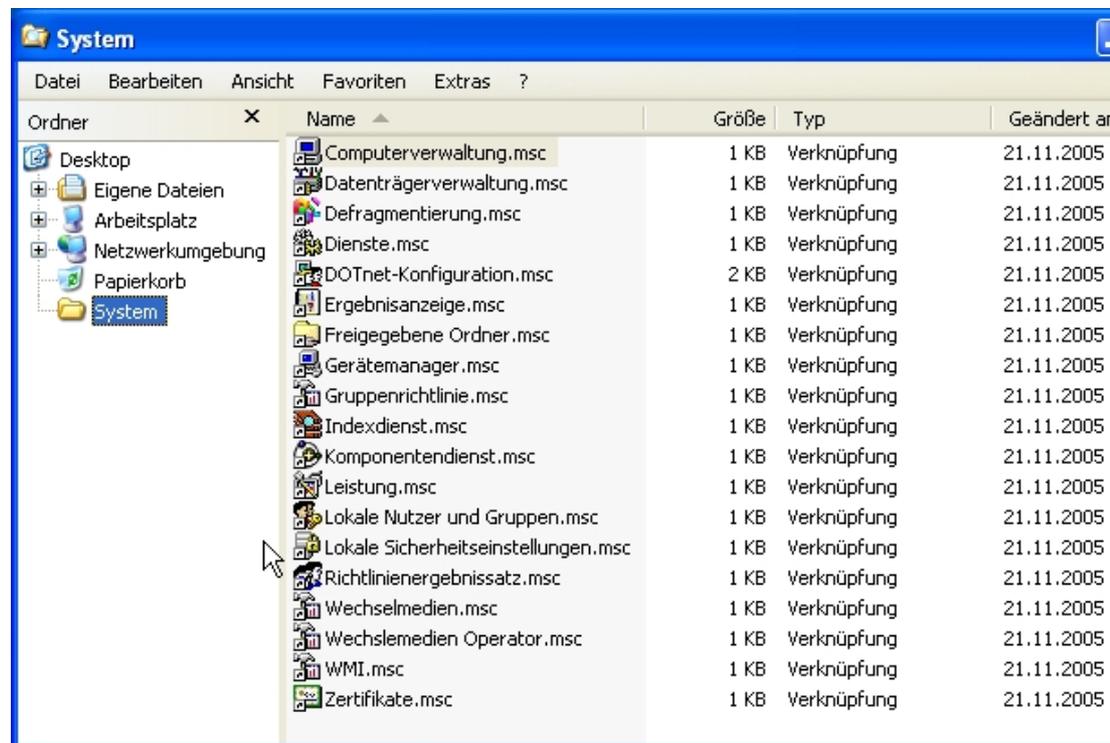
Bislang habe ich zwei Programme gefunden, die auf Administrator-Rechten bestehen:

1. MyTraveler 1.5.7
2. Tivoli Storage Manager Client 5.3.14

MyTraveler ist eine Anwendung, die meinen verschlüsselten Kingston-USB-Memorystick als Laufwerk einbindet. Der TSM-Client sichert alle Daten meiner Workstation und restauriert sie, wenn es nötig ist.

Fazit

Ich fühle mich wohl als „nur“-Hauptbenutzer. Die paar Problemfälle stören in der täglichen Arbeit wenig. Man gewöhnt sich relativ schnell daran, sich bei Bedarf die nötigen Rechte zu verschaffen. Zur Unterstützung meines Gedächtnisses habe ich auf meinem Desktop einen Ordner „System“ angelegt, der Verknüpfungen zu Windows-Dienstprogrammen enthält, die Administrator-Rechte erfordern:



Ausblick

Ich hätte mutiger sein sollen und mich gleich im ersten Schritt mit **Benutzer**-Rechten begnügen sollen. Schließlich garantiert Microsoft erst ab der Beschränkung auf **Benutzer**-Rechte ein sicheres System. Aber solange Viren harmlos sind, wenn sie keine Systemrechte haben und die Mehrrechte des **Hauptbenutzers** nicht gezielt ausnutzen, kann dieser letzte Schritt vielleicht noch warten. Vielleicht aber auch nicht: Es gibt den aktuellen Hinweis 825069 des Microsoft-Supports von Ende November 2005, dass sich **Hauptbenutzer** unter gewissen Umständen Administrator-Rechte verschaffen können. Im Moment gäbe es zwar noch keine Viren, die sich diese Schwachstelle zu nutzen machen würden, aber man könne es auch nicht ausschließen.

Also, seien sie mutiger als ich, und arbeiten gleich nur noch als **Benutzer**!

ZIVGrid – Grid-Computing mit Condor

Martin Leweling

Aufmerksame inforum-Leser dürften es bereits wissen: Grid-Computing ist auf dem Vormarsch. Nach dem Morfeus-Grid der IVV NWZ (inforum-Jubiläumsausgabe 2004) hat jetzt das ZIV mit einem eigenen Condor-Pool nachgezogen.

Angenommen, Sie haben ein Programm für eine Simulation geschrieben, das drei variable Parameter enthält. Für jeden der drei Parameter wollen Sie 10 verschiedene Werte testen, und jeder einzelne Testlauf dauert 3 Stunden. Sie wollen aber nicht wirklich 4 Monate warten, bis Sie auf Ihrem Arbeitsplatzrechner alle Ergebnisse zusammen bekommen und nebenbei auch noch Ihr Rechner für alltägliche Arbeiten viel zu langsam wird. In diesem Fall ist Grid Computing genau das Richtige für Sie.

Das ZIVGrid stellt nun einfach die zumeist ungenutzte Rechenkapazität der ZIVPool-Rechner zur Verfügung, und zwar unter dem Betriebssystem Linux. Im Moment sind dabei die 16 Rechner des ZIVPools 2 nachts ab 17:30 Uhr bis zum nächsten Neustart unter Windows sogar dediziert am ZIVGrid beteiligt, während die Rechner des ZIVPool 3 sich nur dann dem Grid anschließen, wenn sie gerade unter Linux laufen.

Da die Funktionsweise der Grid-Software Condor bereits an anderer Stelle (siehe Artikel über Morfeus in der inforum-Jubiläumsausgabe 2004 unter <http://www.uni-muenster.de/ZIV/inforum/jubilaem-2004/a24.html>) hinreichend erläutert wurde, soll hier nur auf die Besonderheiten und Unterschiede des ZIVGrid im Vergleich zum Morfeus-Grid eingegangen werden. Da gilt es im Wesentlichen, zwei Unterschiede zu beachten: Dies betrifft zum einen die Art des Zugangs, zum anderen die Aufbereitung von Programmen, die im Grid rechnen sollen.

Um im ZIVGrid rechnen zu können, muss man sich zunächst einmal einen Zugang zum Rechner ZIVcluster freischalten, was durch eine Eingabe der Benutzerkennung und des zentralen Passworts in das Web-Formular unter <https://user.uni-muenster.de/exec/zivuseradd.php> geschieht. Näheres zum ZIVcluster können Sie auf den entsprechenden Webseiten unter <http://www.uni-muenster.de/ZIV/Server/ZIVcluster/index.html> nachlesen. Da sowohl der Cluster als auch das ZIVGrid unter Linux betrieben werden, sind für die Nutzung beider natürlich Linux-Kenntnisse Voraussetzung. Der Zugang zum ZIVcluster erfolgt über Secure Shell („ssh“); Dateitransfers kann man entsprechend mit Secure Copy („scp“) oder Secure FTP („sftp“) durchführen. In der Regel werden Sie Ihren Programmtext und Eingabedateien auf den Rechner ZIVcluster transferieren. Natürlich können Sie dort auch auf die unter Linux gewohnten Editoren wie vi, emacs, joe oder nedit zurückgreifen.

Zum Übersetzen Ihres Programmcodes müssen Sie das Kommando `condor_compile <compiler> [options/files ...]` verwenden, wobei `<compiler>` für einen der installierten Compiler/Linker steht: gcc, g++, g77, ld, pgcc, pgf77 oder pghpf. Das folgende Beispiel für den Portland-Fortran-77-Compiler erzeugt die ausführbare Datei `programm.exe` unter Optimierung des Programmcodes für Intel-Xeon- bzw. Pentium-4-Prozessoren:

```
condor_compile pgf77 -tp p7 -fast -o programm.exe programm.f
sub1.f sub2.f ...
```

Dieses Vorgehen stellt den zweiten wesentlichen Unterschied zum Morfeus-Grid der IVV NWZ dar. Die Ursache liegt in der Verwendung verschiedener Ausführungsumgebungen der Condor-Software: Condor kennt unter anderem ein „Standard Universe“ und ein „Vanilla Universe“. Das „Standard Universe“ unterstützt *checkpointing* und *remote system calls*, was bedeutet, dass der Zustand eines Condor-Jobs in regelmäßigen Abständen „eingefroren“ wird und der Prozess vom aktuellen Rechner auf einen anderen migriert werden kann. Im Prinzip ist es somit möglich, auch wochenlange Berechnungen im ZIVGrid durchzuführen, selbst wenn die Rechner tagsüber mit ganz anderen Dingen beschäftigt sind und sogar mehrfach neu gestartet werden. Dafür gibt es eine ganze Reihe von Einschränkungen bei der Art von Prozessen, die im „Standard Universe“ gestartet werden können. So sind z. B. Mehrprozess-Jobs ausgeschlossen, also etwa die Verwendung von `fork()`, `exec()` oder `system()`. Das Morfeus-Grid hingegen unterstützt ausschließlich das „Vanilla Universe“, das zwar weniger Limitierungen bei der Jobauswahl mitbringt, aber eben den Abbruch eines Jobs und Neustart auf einem anderen Rechner erzwingt, wenn der aktuell verwendete Rechner einen Reboot durchführt.

Bevor man nun einen Job in die Condor-Warteschlange abschicken kann, muss man zunächst ein sogenanntes „Submit description file“ schreiben. Das kann für den Anfang so einfach aussehen wie:

```
Executable = programm.exe  
Log = programm.log  
Queue
```

Im Prinzip sind die „Executable“- und „Queue“-Zeilen die einzigen Pflicht-Einträge in dieser Datei. Hat man das Beispiel etwa in der Datei `programm.cmd` gespeichert, kann man den Job mit dem Kommando

```
condor_submit programm.cmd
```

in das ZIVGrid abschicken. Mit `condor_q` kann man sich dann die Queue oder mit `condor_status` den Zustand jedes Rechners im Grid anschauen. Sobald der Rechenjob beendet ist, landen die Ergebnisse in genau demselben Verzeichnis, aus dem heraus der Job abgeschickt worden ist, üblicherweise also innerhalb des eigenen Heimatverzeichnisses auf dem ZIVcluster.

Weitergehende Informationen zum ZIVGrid finden Sie unter der URL <http://www.uni-muenster.de/ZIV/Server/ZIVGrid>. Dort gibt es neben dem vollständigen Condor-Benutzerhandbuch eine tabellarische Befehlsübersicht sowie eine Kurzeinführung für Nutzer, die nicht gerne lange Bedienungsanleitungen lesen.

Im Moment befindet sich das ZIVGrid noch in einer Testphase. Allerdings werden dringend testwillige Nutzer benötigt, da nur so eine optimale Konfiguration des ZIVGrids erreicht werden kann und Fehler in der Konfiguration natürlich nur bei hinreichender Nutzung auffallen. Dabei sollten sich also insbesondere solche Nutzer angesprochen fühlen, die den Linux-Parallelrechner ZIVcluster bislang hauptsächlich für serielle Programme genutzt haben und nicht auf Spezial-Software (wie z. B. Gaussian) angewiesen sind.

ZIV-Lehre

ZIV-Lehre wird geschätzt

W. Bosse

Ergebnis der Evaluation des Lehrangebots

Der von der IV-Kommission eingesetzte IV-Lehrausschuss hat in der Kommissionsitzung im November 2005 einen Bericht zur Evaluation des Lehrangebots des Zentrums für Informationsverarbeitung (ZIV) gegeben und dabei die ZIV-Lehre positiv gewürdigt. Unter Berücksichtigung der Tatsache, dass die Veranstaltungen von Studierenden aus mehreren Fakultäten besucht werden, die unterschiedliche Vorkenntnisse aufweisen, ist dies natürlich besonders erfreulich. Wörtlich heißt es in dem Bericht: „Die Präsentation des Stoffes, die Kompetenz der Dozenten (teilweise mit Höchstnote) und die sehr guten Lernfortschritte werden von den Teilnehmern durchweg gelobt.“

Dieses Ergebnis ist für die in der IV-Lehre engagierten Wissenschaftlichen Mitarbeiter des ZIV Lob und Ansporn zugleich. So sind für das Frühjahr 2006 und das kommende Sommersemester auch bereits wieder Lehrveranstaltungen aus den Themenbereichen Programmiersprachen, Betriebssysteme, Netze und Spezialanwendungen geplant, zu denen Interessenten sich jeweils zeitnah, i. d. R. etwa 6 Wochen im Voraus, ausgehend von der Webadresse <http://www.uni-muenster.de/ZIV/Lehre/index.html> anmelden können (siehe dazu auch die kommentierte Zusammenstellung in dieser **inforum**-Ausgabe).

Veranstaltungen in der vorlesungsfreien Zeit (Frühjahr 2006) für Hörer aller Fachbereiche

Beratung zum Lehrangebot durch Herrn W. Bosse jeweils Di, Do 11–12, ☎83-3 15 61

Für alle Veranstaltungen ist eine frühzeitige Online-Anmeldung erforderlich, die ausgehend von der Webadresse <http://www.uni-muenster.de/ZIV/Zivlehre.html> erfolgen kann. Für den Dialog sollte dabei vorzugsweise auf die dort angebotene verschlüsselte (abhörsichere) Datenübertragung umgeschaltet werden. Anmeldungen zu den Veranstaltungen sind möglich ab 9. Januar 2006 für die vorlesungsfreie Zeit. Weitere Informationen unter <http://www.uni-muenster.de/ZIV/Lehre/>.

260010	Programmieren in Java vom 06.03. bis 17.03.2006, Mo-Fr 10-17 Uhr Hörsaal: M4, Einsteinstr. 64	Mersch, R.
260024	Programmieren in Java für Fortgeschrittene vom 20.03. bis 31.03.2006, Mo-Fr 9-11 Uhr Hörsaal: M4, Einsteinstr. 64	Süselbeck, B.
260039	Multimedia Praktikum vom 13.02. bis 24.02.2006, Mo-Fr 9-16 Uhr Hörsaal: Multimedia-Räume, Einsteinstr. 60	Scheffer, A.
260043	Betriebssystem Linux/Unix: Einführung und Grundlagen vom 28.02. bis 10.03.2006, Mo-Fr 10-16 Uhr Hörsaal: ZIV-Pool 3, Einsteinstr. 60 Beginn: Dienstag, 28.02.2006	Grote, M.
260058	Systemadministration für Linux-Systeme vom 27.03. bis 31.03.2006, Mo-Fr 9-16 Uhr Hörsaal: ZIV-Pool 3, Einsteinstr. 60	Hölters, J.

- 260062 Administration eines Windows-Systems** Kämmerer, M.
vom 20.02. bis 24.02.2006, Mo-Fr 9-16 Uhr
Hörsaal: ZIV-Pool 3, Einsteinstr. 60
- 260077 Systemadministration für Windows-Server in einer Active Directory Umgebung** Lange, W., Winkelmann, O.
vom 20.03. bis 24.03.2006, Mo-Fr 10-16 Uhr
Hörsaal: ZIV-Pool 3, Einsteinstr. 60

Kommentare zu den Veranstaltungen

260010 Programmieren in Java

Java ist eine objektorientierte Programmiersprache, die inzwischen weltweit große Verbreitung gefunden hat und sich weiterhin dynamisch entwickelt. Sie basiert auf dem Konzept einer virtuellen Maschine, die es ermöglicht, Anwendungen für unterschiedliche Plattformen ohne Neuübersetzung zu entwickeln, und verfügt über eine sehr umfangreiche Klassenbibliothek, die ständig erweitert wird. Grundkenntnisse in Java sind für die Softwareentwicklung in vielen Bereichen unbedingt erforderlich.

Die Vorlesung bietet eine Einführung in die objektorientierte Programmierung anhand von Java. Sie ist auch für Hörer/innen ohne Vorkenntnisse im Programmieren geeignet.

260024 Programmieren in Java für Fortgeschrittene

In der Vorlesung sollen einige fortgeschrittene Konzepte der Programmiersprache Java vorgestellt werden. Am Anfang der Lehrveranstaltung stehen Techniken zur Unterstützung der parallelen Programmierung (Multithreading) in Java. Im Anschluss daran erfolgt eine Übersicht zu Input/Output in Java (Streams-Konzept). Als internetbasierte Sprache bietet Java eine Reihe von Werkzeugen zur Netzwerkprogrammierung. Neben der Vorstellung der entsprechenden Grundlagen erfolgt eine Übersicht zu den darauf aufbauenden Themen wie Remote Method Invocation, Datenbankzugriff und Servlets. Einen weiteren Themenschwerpunkt bilden schließlich neuere Konzepte zur Gestaltung grafischer Benutzeroberflächen wie Java-Beans und die Swing-Klassen.

260039 Multimedia Praktikum

Das Praktikum führt in die elementaren Techniken der Bildgewinnung und deren Präsentation ein. Es besteht aus einem vorbereitenden theoretischen Teil, der vorab im Internet veröffentlicht wird, und einem Praktikumsteil. Im theoretischen Teil werden unter andere folgende Themen behandelt:

- Die Grundlagen der Gewinnung eines digitalen Fotos (Bayer-Muster)
- Algorithmen zur Umwandlung von Bayer-Mustern in Fotos
- Die Qualität digitaler Bilder (Modular Transfer Function)
- Grundlagen der Farbenlehre
- Bildbearbeitungsalgorithmen (Farbumfang, Schärfung usw.)
- Bildformate (Jpeg, Tiff, Gif usw.)
- Kurzeinführungen in die verwendeten Standardprogramme (Photoshop, Acrobat usw.)
- Schrittweise Arbeitsanleitungen für die Experimente des praktischen Teils

Im praktischen Teil werden die Hörer/innen Erfahrung im Umgang mit Flachbett-Scannern, Dia-Scannern, digitalen Kameras, Videokameras und Webcams gewinnen. Gleich-

zeitig wird auch die Präsentation des gewonnenen Bildmaterials als Druckausgabe, Photo-CD, Video-CD und DVD trainiert. In Experimenten wird behandelt:

- Die Gewinnung von gerasterten Bildern (von Druckvorlagen); Gerät: Flachbettscanner; Präsentation: Druck
- Die Gewinnung von Bildern mit kontinuierlicher Farbverteilung (von Photos); Gerät: Dia-Scanner; Präsentation: Druck
- Die Bildgewinnung mit einer digitalen Kamera; Präsentation: Still-Video-CD
- Die Bildgewinnung mit einer digitalen Video-Kamera (d. h. Filmerstellung); Präsentation: Video-CD
- Die Durchführung einer Video-Konferenz; Gerät: Webcam; Präsentation: Bildschirm

Die Teilnehmer des Praktikums arbeiten bei diesen Experimenten in den Multimedia-Räumen des ZIV und in Gruppen von maximal drei Personen. Die Experimente werden von den Mitarbeitern des ZIV betreut. Dem praktischen Teil angegliedert sind Einführungen zu den Themen:

- Filmsprache und -gestaltung (findet im Servicepunkt Film statt)
- Digitaler Videoschnitt an professionellen Schnittplätzen (findet im Servicepunkt Film statt)
- Digitale Spiegelreflex-Fotografie

Die Teilnehmer des Praktikums legen ein Praktikumsbuch an. Das Praktikum erfordert eine Voranmeldung. Auf Grund der eingeschränkten Räumlichkeiten ist die Teilnehmerzahl beschränkt. Entscheidend für die Teilnahme am Praktikum ist neben der Online-Anmeldung die Anwesenheit am ersten Praktikumstag, an dem die Gruppen eingeteilt werden.

260043 Betriebssystem Linux/Unix: Einführung und Grundlagen

Linux ist ein leistungsstarkes Unix-System für viele Hardware-Architekturen, das sich als preiswerte Windows-Alternative etabliert hat. Die Vorlesung will in die Linux-Benutzung einführen. Neben einer an üblichen Unix-Einführungen orientierten Beschreibung des Unix-Datei-Systems und der wesentlichen Unix-Befehle wird die grafische Oberfläche KDE behandelt, die für viele ein Linux-System erst attraktiv macht.

260058 Systemadministration für Linux-Systeme

Die Vorlesung richtet sich an fortgeschrittene Linux-Anwender/innen, die Unterstützung bei der Installation und System-Integration von Linux-Systemen benötigen. Voraussetzung sind grundlegende Kenntnisse der Unix-Kommandos. Die Teilnehmer/innen werden in der Veranstaltung ein Linux-System selbst installieren und in die Netzwerk- und Systeminfrastruktur der Universität einbinden, dazu gehört die Nutzung eines Verzeichnisdienstes für die Account- und Nutzerinformation, sowie die Nutzung eines Kerberosdienstes zu Authentisierung. Ferner wird auch die automatisierte Installation und Parametrierung einer größeren Anzahl von Linux-Systemen behandelt.

260062 Administration eines Windows-Systems

Für Hörer/innen mit Windows-Vorkenntnissen werden Aufbau und Betrieb von Windows XP und Windows Server 2003 vorgestellt und gemeinsam erprobt. Die folgenden Themen werden u. a. Behandelt:

- Installation des Betriebssystems und Absicherung gegen Angriffe von außen
- Zugriffsrechte und Netz-Freigaben
- Benutzer- und Gruppenverwaltung, lokale Administration
- Druck-, Datei-, Logon- und allgemeine Programm-Services

- Diagnose- und Überwachungsfunktionen
- Internet, LAN, Netz-Protokolle

Die speziellen Dienste E-Mail-, Datenbank-, Web- und Media-Server können im Rahmen dieser Veranstaltung nicht bearbeitet werden. Die Einbindung in eine Windows Active Directory Domäne wird nur am Rande erwähnt. Wir verweisen auf die weitere Veranstaltung „Systemadministration für Windows-Server in einer Active-Directory-Umgebung“.

260077 Systemadministration für Windows-Server in einer Active-Directory-Umgebung

Die Veranstaltung richtet sich an fortgeschrittene Windows-Benutzer, die ihre Kenntnisse mit Blick auf die Anforderungen in einem großen Rechnernetz erweitern möchten. Als Schwerpunkte sind u. a. der Aufbau und Betrieb von Servern in einer Active-Directory-Umgebung (Windows-Netzwerk) vorgesehen.

Themenauswahl:

- Installation und Konfiguration
- Benutzerverwaltung
- Sicherheit u. a.: Dateisystem, Registry, Netzwerk, Sicherheitsrichtlinien
- Server im Active Directory: Gesamtstrukturen, Domänenstrukturen, Domänen, Organisationseinheiten (OU), Vertrauensstellungen, Standorte, Replikation, Gruppenrichtlinien
- Softwareverteilung und Systemüberwachung

Im Rahmen der Veranstaltung wird auch Gelegenheit zu praktischen Übungen gegeben.

ZIV-Regularia

Fingerprints

R. Perske

Unter dieser Rubrik erscheinen regelmäßig die aktuellen kryptographischen Prüfsummen der Zertifizierungsstelle der Universität Münster (WWUCA).

Viele Server in der Universität (WWW, E-Mail, NetNews usw.) bieten per SSL/TLS geschützte Zugänge an, damit Passwörter und Daten bei der Übertragung vor unbefugtem Mitlesen geschützt sind. Beim Verbindungsaufbau weisen diese Server ihre Identität durch Zertifikate nach, welche von der Zertifizierungsstelle der Universität Münster (WWUCA) ausgestellt sind. Normalerweise wird Ihre Software diese Zertifikate nicht überprüfen können und lästige Warnmeldungen ausgeben.

Um diese Warnmeldungen zu deaktivieren, sollten Sie einmalig das CA-Zertifikat der WWUCA in Ihre Software integrieren. Dazu gehen Sie einfach auf die WWW-Seite <http://permail.uni-muenster.de> und klicken Sie dort nacheinander auf Schritt 1 und auf Schritt 2. Ihr WWW-Browser wird jeweils Dialogboxen präsentieren. Damit öffnen (nicht speichern) Sie die Datei und installieren Sie das Zertifikat; je nach Software müssen Sie dazu Buttons drücken oder Häkchen setzen. Um sicher zu gehen, dass Ihnen kein falsches CA-Zertifikat untergeschoben wird, sollten Sie dabei den Fingerabdruck des CA-Zertifikats mit den unten bei den X.509-Zertifikatdaten abgedruckten Fingerabdrücken vergleichen.

Auch bei E-Mails wird immer mehr mit Verschlüsselung und elektronischen Unterschriften gearbeitet. Angehörige der Universität und des Universitätsklinikums können ihre S/MIME- und PGP-/GnuPG-Schlüssel durch die WWUCA zertifizieren lassen. Mit den nachfolgenden Fingerprints können auch die Echtheit dieser Zertifikate überprüfen.

Weitere Informationen zur Zertifizierung erhalten Sie unter <http://www.uni-muenster.de/wwuca/>. Ab dem neuen Jahr wird die WWUCA den neuen DFN-PKI-2-Dienst der DFN-PCA nutzen, dadurch ändert sich das Verfahren für X.509-Zertifikate. Ein komplett überarbeiteter Webauftritt mit genauere Informationen auch zu diesem Thema wird ab Januar unter dieser Adresse zu finden sein.

PGP-Kommunikationsschlüssel

Da die Zertifizierungsschlüssel ausschließlich zum Zertifizieren verwendet werden, gibt es gesonderte Kommunikationsschlüssel, die Sie bitte verwenden, wenn Sie eine verschlüsselte E-Mail an die jeweilige Zertifizierungsstelle schreiben möchten:

Zertifizierungsstelle Universitaet Muenster (E-Mail) ca@uni-muenster.de
 KeyID 4CB7658D, 2048 Bits, Fingerprint: 383D 0F16 CEFC 1F9E B7C3 04B1 2020 FCE6

DFN-PCA (2005), ENCRYPTION Key dfnpca@dfn-cert.de
 KeyID: 13813809, 2048 Bits, Fingerprint: 53C2 37D6 155B CF88 F37D 3FF5 E2E4 E51D

PGP-Zertifizierungsschlüssel der WWUCA

Zertifizierungsstelle Universitaet Muenster 2006-2007
 KeyID: 31027DB5, 2048 Bits, Fingerprint: A57B 0407 1F91 9CB9 3771 3736 E195 6C62

Zertifizierungsstelle Universitaet Muenster 2004-2005
 KeyID: 38B7A481, 2048 Bits, Fingerprint: 973E 0725 040B 1745 F272 180D 08C2 C15A

Zertifizierungsstelle Universitaet Muenster 2002-2003
 KeyID: BC811EB1, 2048 Bits, Fingerprint: 2864 01BC F0EF D5BA D9A0 866C 4379 4C1D

Zertifizierungsstelle Universitaet Muenster 2000-2001
 KeyID: 313C02F5, 2048 Bits, Fingerprint: 3762 F5E0 C278 7697 530F 2DF2 F3B3 27F5

Rainer Perske +49(251)83-31582 Certification Key
 KeyID: EF750F1D, 2048 Bits, Fingerprint: 2F38 6EF8 DC2E D85E 5B35 DB49 8AE4 52AF

PGP-Zertifizierungsschlüssel der DFN-PCA:

Der Schlüssel für 2006-2007 lag bei Redaktionsschluss noch nicht vor.

DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2004-2005) <http://www.dfn-pca.de/>
KeyID: FDCB1C33, 2048 Bits, Fingerprint: 96B0 AD7F B8DC 0018 DCA0 7053 1C3B 4DA5

DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2002-2003) <http://www.dfn-pca.de/>
KeyID: F2D58DB1, 2048 Bits, Fingerprint: DE31 690D BC6A E779 4DCD A1B5 8180 FE7B

DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2001) <not-for-mail>
KeyID: 63EB5391, 2048 Bits, Fingerprint: CFAF 6C29 4E57 4E0E E81C BDB4 54FD 2AAB

DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 1999-2000) <not-for-mail>
KeyID: F7E87B9D, 2048 Bits, Fingerprint: 6570 7274 B5E0 3FF0 EA7C ABE4 465F B8B2

DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 1997-1998) <not-for-mail>
KeyID: 35DBF565, 2048 Bits, Fingerprint: 097C 0919 D3C3 86DC 7A30 1511 1295 8DE3

X.509-Zertifikatdaten der WWUCA

Die Zertifikatdaten für 2006-2007 lagen bei Redaktionsschluss noch nicht vor.

C=DE, O=Universitaet Muenster, CN=Zertifizierungsstelle 2004-2005/Email=ca@uni-muenster.de
MD5-Fingerprint: 2619 6bef 66b2 7044 52cc be11 4c5f 3cb8
SHA1-Fingerprint: 1765 ae6d 57c7 7914 d2af baf3 439c e139 66e1 a0ae

C=DE, O=Universitaet Muenster, CN=Zertifizierungsstelle 2002-2003/Email=ca@uni-muenster.de
MD5-Fingerprint: a431 ad41 d8f2 1856 4e31 cc69 71e6 174f
SHA1-Fingerprint: 6945 20ca 1afe 5cfa 6c37 52eb b772 b054 90ec d979

X.509-Zertifikatdaten der DFN-PCA

C=DE, O=DFN-Verein, OU=DFN-PKI, CN=DFN-Verein PCA Classic - G01
MD5-Fingerprint: EF08 E69F 6AC7 252C 588C 55FD 4513 310A
SHA1-Fingerprint: 1263 4160 D08C FE6A 876D F786 D3AD C2F7 74FF 219F

C=DE, O=DFN-Verein, OU=DFN-PKI, CN=DFN-Verein PCA Basic - G01
MD5-Fingerprint: 7695 48F0 4072 3C2B A6A1 A1FD CCAF 7FF4
SHA1-Fingerprint: 355E 6967 8EB5 D72B 5DC8 8227 6847 F27C 0D3C 4156

C=DE, O=DFN-Verein, OU=DFN-PKI, CN=DFN-Verein PCA Grid - G01
MD5-Fingerprint: 4139 4A58 2EF0 45B2 2928 F172 ABF7 0508
SHA1-Fingerprint: 1CBB D4BA 977B 3AB9 FFCD 4A97 7750 879C 6A2E 8E38

C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA,
CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
MD5-Fingerprint: 3e1f 9ee6 4c6e f022 0825 da91 2308 050
SHA1-Fingerprint: 8e24 22c6 7e6c 86c8 90dd f69d f5a1 dd11 c4c5 ea81

Ausgewählte X.509-Server-Zertifikate

Leider ist es für die meisten Nutzer zu schwierig, die CA-Zertifikate auch in Ihrem E-Mail- oder NetNews-Programm zu installieren. Um Ihnen die Überprüfung der Zertifikate unserer E-Mail-Server zu erleichtern, drucken wir hier zusätzlich die Fingerprints der entsprechenden Server-Zertifikate ab:

IMAP-Server imap.uni-muenster.de (eingehende E-Mail, E-Mail-Ordner):

C=DE, O=Universitaet Muenster, OU=Zentrum fuer Informationsverarbeitung,
CN=imap.uni-muenster.de/emailAddress=wwwadmin@uni-muenster.de
MD5-Fingerprint: 7B89 EC4D 005B 91D6 EAED 3390 B06B B75E
SHA1-Fingerprint: F149 6618 1015 9E90 3F8E 3F28 03A9 7073 BDCF DEE3

POP3-Server pop.uni-muenster.de (eingehende E-Mail):

C=DE, O=Universitaet Muenster, OU=Zentrum fuer Informationsverarbeitung,
CN=pop.uni-muenster.de/emailAddress=wwwadmin@uni-muenster.de
MD5-Fingerprint: 9520 2C42 71EA 5550 164C 8820 F082 46F6
SHA1-Fingerprint: B78F EADC B65A 83B8 C43E F8C8 4C60 37EC CAFC 0D00

SMTP-Server secmail.uni-muenster.de (ausgehende E-Mail):

C=DE, O=Universitaet Muenster, OU=Zentrum fuer Informationsverarbeitung,
CN=secmail.uni-muenster.de/emailAddress=wwwadmin@uni-muenster.de
MD5-Fingerprint: 083E 1614 847C A973 B023 6FB3 468A BF74
SHA1-Fingerprint: 10FE BDFC 16F5 86E2 F84D 3FB7 0B0A 1383 2354 1D3B

NNTP-Server news.uni-muenster.de (NetNews):

C=DE, O=Universitaet Muenster, OU=Zentrum fuer Informationsverarbeitung,
CN=news.uni-muenster.de/emailAddress=wwwadmin@uni-muenster.de
MD5-Fingerprint: 2D33 9791 FE28 6B88 45A6 3D22 69AF 1017
SHA1-Fingerprint: EE99 B4D4 A96C 5254 7145 2085 761D 8176 E1DD 0144

Liebe Leserin, lieber Leser,

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

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

Vielen Dank!

Redaktion **inforum**



-
- Ich bitte um Aufnahme in den Verteiler.
 - Bitte streichen Sie mich/den nachfolgenden Bezieher aus dem Verteiler.
 - Mir reicht ein Hinweis per E-Mail nach dem Erscheinen einer neuen WWW-Ausgabe.
Meine E-Mail-Adresse:

┌ An die
Redaktion **inforum**
Zentrum für Informationsverarbeitung
Röntgenstr. 9-13
48149 Münster

- └
- Meine Anschrift hat sich geändert.
Alte Anschrift:

└

└

Absender: Name: _____ FB: _____ Institut: _____ Straße: _____ E-Mail: _____ Außerhalb der Universität: _____
--

(Bitte deutlich lesbar in Druckschrift ausfüllen!)

Ich bin damit einverstanden, dass diese Angaben in der **inforum**-Leserdatei gespeichert werden (§ 4 DSGVO).

Ort, Datum

Unterschrift