

inforum

Zentrum für Informationsverarbeitung der Universität Münster
Jahrgang 28, Nr. 3 – Dezember 2004 ISSN 0931-4008

Inhalt

Editorial	2
ZIV-Aktuell	3
Gigabit-Anbindung des G-WiN-Clusters Münster an das G-WiN/Internet realisiert.....	3
Direkte Verbindung zu den Forschungsnetzen Lateinamerikas.....	4
ZIV unterstützt Radio Q.....	5
Intro – Schließenanlagen im ZIV und anderswo.....	5
Erste Schritte zur Einführung eines Identity-Managements an der WWU.....	8
Zur Sonderausgabe inforum	10
Neues von perMail.....	13
Spam-Entsorgung mit perMail.....	14
AutoDeleatur.....	19
Neues zum SPSS.....	19
Suchmaschinen an der Universität Münster.....	20
Uni Münster setzt auf SIP.....	21
VPN-Verbindungen mit Firewall unter Linux.....	23
Nutzung öffentlicher und privater Subnetze im LAN der Universität.....	25
DFNVC – der Videokonferenzdienst im deutschen Wissenschaftsnetz.....	27
Die neuen Multimedia-Räume des ZIV.....	28
ZIV-Lehre	32
Veranstaltungen in der vorlesungsfreien Zeit (Frühjahr 2005).....	32
Veranstaltungen in der Vorlesungszeit (Sommersemester 2005).....	33
Kommentare zu den Veranstaltungen.....	33
ZIV-Regularia	37
Fingerprints.....	37



Impressum

infoforum
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
(Rank Xerox DocuTech 135)

Auflage dieser Ausgabe: 1400

Editorial

E. Sturm



Durch ein glückliches Zusammentreffen erscheinen jetzt zwei Ausgaben unserer Informationsschrift **infoforum** gleichzeitig und damit rechtzeitig zu den Tagen zwischen den Jahren, wo man vielleicht etwas mehr Zeit zum Lesen hat: Die Sonderausgabe zum 40-jährigen Jubiläum des ZIV (vormals Universitätsrechenzentrum), zum 20-jährigen des Uni-Netzes (LAN) und zum 20-jährigen des Computer-Investitions-Programms (CIP) und zum anderen die reguläre dritte **infoforum**-Ausgabe dieses Jahres.

Erschien es zunächst so, dass die Sonderausgabe der regulären die Autoren wegnahm, so kam es dann doch anders. Am Inhaltsverzeichnis der Sonderausgabe, das wir in dieser Ausgabe kommentiert abdrucken, sehen Sie, dass dort eher Artikel grundsätzlicher Art, oft dazu von Autoren außerhalb des Hauses enthalten sind. Auch die Grußworte sind vielsagender, als man zunächst denkt.

In dieser Ausgabe finden Sie sowohl Artikel zu konkreten Vorhaben des ZIV (Identitäts-Management, Multimediaräume, Intro, perMail, Deleatur) als auch Artikel zu Entwicklungen außerhalb des ZIV wie Voice-over-IP und Video-Konferenzen (über den DFN-Verein).

Speziell Voice-over-IP verspricht, international gesehen, Stoff für weitere Editorials abzugeben. Wenn Telefonieren erst kostenlos ist, wird man bestimmt nachts öfter aus Indien angerufen und gefragt, ob man Vigaga oder etwas Ähnliches haben möchte. In diesem Zusammenhang können Sie sich schon mal das Wort Spit (Spam über Internet-Telefon) merken. Dagegen wird es dann Spracherkennungssysteme geben, denen ein Anrufer so lange sein Anliegen schildern muss, bis die Spitzwahrscheinlichkeit unter 10 % gesunken ist.

ZIV-Aktuell

Gigabit-Anbindung des G-WiN-Clusters Münster an das G-WiN/Internet realisiert

Markus Speer

Seit dem 30.9.2004 ist das G-WiN-Cluster Münster mit einer Bandbreite von 1 Gigabit pro Sekunde (bisher 155 Megabit/s) an das G-WiN/Internet angeschlossen. Der Anschluss erfolgt über eine 112 km lange Glasfaserverbindung zum nächsten G-WiN-Anschlussknoten in Essen. Diese Art der sehr flexiblen Weitverkehrsverbindung ist derzeit einzigartig im DFN.

Bei der zwischen Essen und Münster realisierten Glasfaserverbindung handelt es sich als Besonderheit um eine sog. „Dark Fiber“, d. h. eine durchgehende, reine Glasfaserverbindung ohne irgendwelche aktive Netztechnik. Als Netztechnologie kommt Gigabit-Ethernet zum Einsatz. Bislang wird im G-WiN für Weitverkehrsverbindungen die klassische sog. SDH-Technologie eingesetzt. Gegenüber dem bisherigen 155-Mbit/s-Hauptanschluss steht nun eine fast 6,5-fache Bandbreite zur Verfügung. Die Glasfaserleitung zwischen Essen und Münster wurde dem DFN-Verein von der Firma GasLINE anlässlich des 20-jährigen DFN-Jubiläums im Juni 2004 überlassen. In Zusammenarbeit mit dem Unternehmen TROPOLYS wurden die Verbindungen innerhalb der beiden Stadtbeiriche realisiert. Die für den Betrieb der – für Gigabit-Ethernet-Verhältnisse extrem langen – Leitung notwendigen speziellen Geräte wurden von der Firma Dimension Data zur Verfügung gestellt. Über die „Dark Fiber“ sollen zusammen mit dem DFN-Verein neben dem Produktionsbetrieb auch alternative Formen von Netzanbindungen und Netzanwendungen erprobt werden. Die neue Verbindung zwischen Münster und Essen ist auch im Zusammenhang mit vorbereitenden Maßnahmen für die nächste Generation des Deutschen Forschungsnetzes, dem X-WiN, zu sehen.

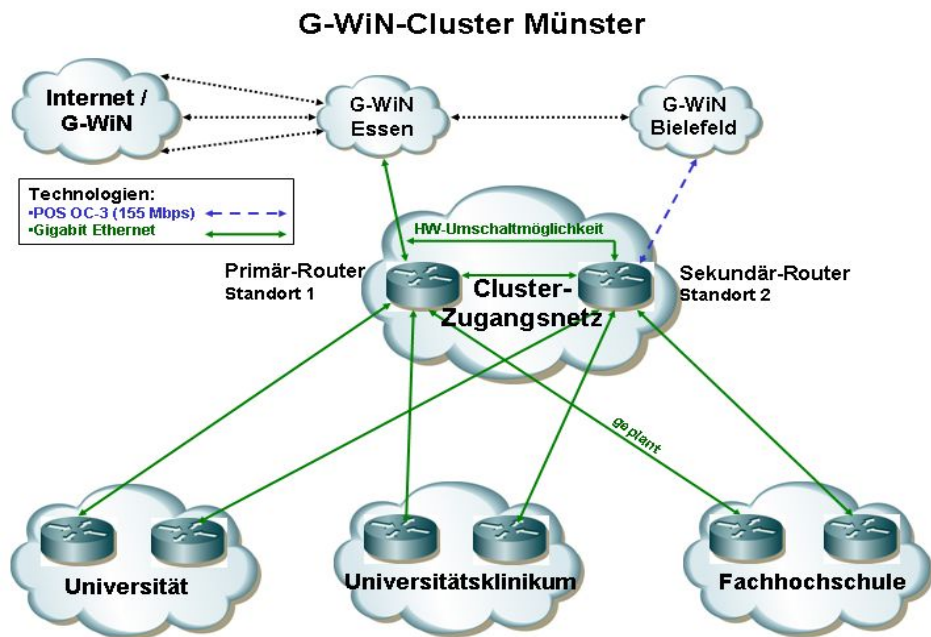


Abb. 1

Vor der Übernahme der „Dark Fiber“-Verbindung in den Produktionsbetrieb wurde die Verbindung zunächst ausgiebig erprobt, um keinerlei Einbußen in der Verfügbarkeit gegenüber der bisherigen G-WiN-Backup-Konfiguration (vgl. Artikel in infoForum Nr. 3/2003) hinnehmen zu müssen. Durch die direkte Primäranbindung an den G-WiN-Kernnetzstandort Essen ist auf jeden Fall die bisher noch gegebene Abhängigkeit vom G-WiN-Standort Bielefeld beseitigt (vgl. Abb. 1). Der mit dem G-WiN-Standort Bielefeld verbundene Sekundäranschluss, der bei Ausfall des Primäranschlusses verwendet wird, wurde am 21.09.2004 von 34 Mbit/s auf 155 Mbit/s hochgerüstet. Durch den Wegfall der 34-Mbit/s-E3-Technologie ist nun auch eine Reduzierung der eingesetzten Netztechnologien erzielt worden, wobei für den Regelbetrieb nun nur noch die Standard-Technologie Gigabit-Ethernet zum Einsatz kommt. Um einen Totalausfall des Pri-

mär-Routers abfangen zu können, existiert weiterhin eine Hardware-Umschaltmöglichkeit des neuen Primär-Anschlusses auf den Sekundär-Router. Der G-WiN-Standort Essen ist redundant (u. a. über eine 10-Gbit/s-Verbindung) in das G-WiN eingebunden (vgl. Abb. 2). Insgesamt ist die Performance und die Verfügbarkeit der Internet-Anbindung für die Universität Münster mit Universitätsklinikum, für die Fachhochschule und das neue Max-Planck-Institut noch einmal deutlich verbessert worden. Betrieben werden die beiden Internet-Anschlüsse vom Zentrum für Informationsverarbeitung (ZIV) der Universität.

Links:

- Betriebsdaten des Wissenschaftsnetz-Anschlusses: <http://www.uni-muenster.de/ZIV/Content--NetzInternetZugangBetriebStatistik.html>

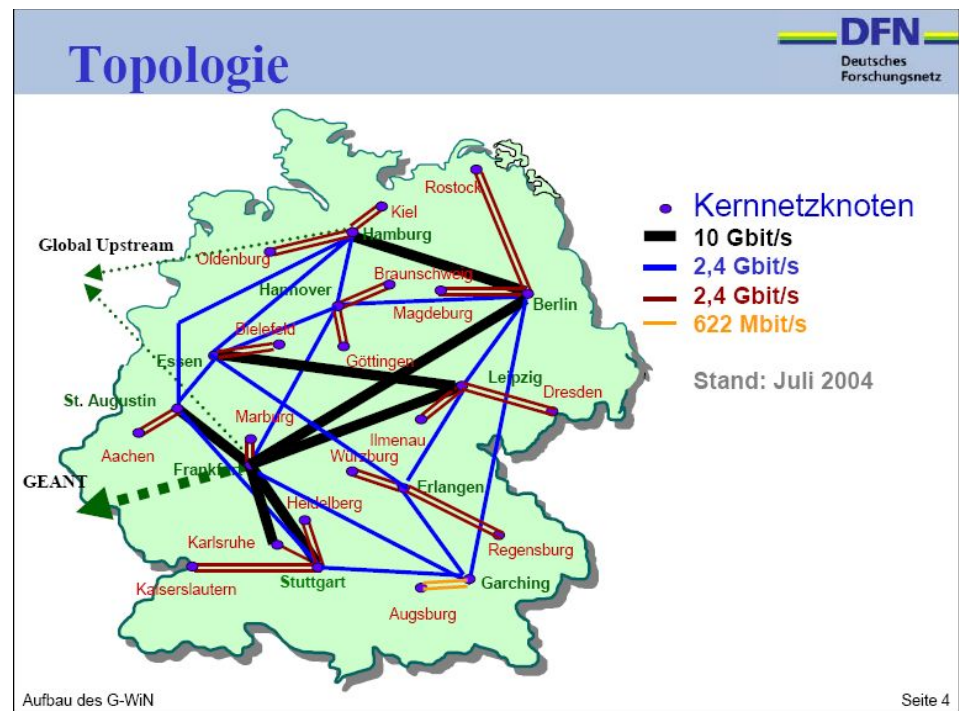


Abb. 2

Direkte Verbindung zu den Forschungsnetzen Lateinamerikas

W. Held

Seit dem 1. August 2004 verbindet der lateinamerikanische Forschungsbackbone ALICE (America Latina Interconectada Con Europa) die Forschungsnetze mehrerer lateinamerikanischer Staaten mit einem 155-Mbit/s-Ring. Im ersten Schritt sind damit die NRENs Argentiniens, Brasiliens, Chiles, Panamas und Mexikos untereinander verbunden. Zusätzlich bietet ALICE eine 622-Mbit/s-Verbindung zum europäischen Forschungsbackbone GÉANT. Das mit 10 Millionen Euro von der EU geförderte Projekt läuft bis April 2006. Weitere Verbindungen werden in Kürze Uruguay, Paraguay und Venezuela mit ALICE verlinken. Weitere Informationen stehen unter <http://www.dante.net/> zur Verfügung.

ZIV unterstützt Radio Q

G. Wessendorf

Die Welt hört auf Münster – Campusradio sendet jetzt auch im Internet.

Seit dem 3. September 2004 wird das Programm von Radio Q über einen leistungsfähigen Server des ZIV über das Universitäts-Rechnernetz und damit auch über das internationale Internet zum Live-Abruf zur Verfügung gestellt. Dazu wurde folgende Pressemitteilung von Radio Q herausgegeben:

Die Welt hört auf Münster – Campusradio sendet jetzt auch im Internet

Münster, September 2004. Wer Radio Q, das Campusradio der münsterschen Hochschulen, einstellen wollte, hörte auf der 90,9 nur Rauschen, wenn die Studentenbude nicht im näheren Umkreis der Universität lag. Damit ist jetzt Schluss: Gemeinsam mit dem Zentrum für Informationsverarbeitung (ZIV) der Westfälischen Wilhelms-Universität bieten die studentischen Radiomacher jetzt den Empfang übers Internet an – weltweit. „Wir haben früher immer viele Anfragen bekommen, wann man Radio Q endlich auch außerhalb der Innenstadt hören könne. Bislang mussten wir hier immer vertrösten“, erinnert sich Daniel Fiene, Technikchef des Campusradios, „Das Internet macht es möglich, dass wir heute niemanden mehr enttäuschen müssen.“

Über die Homepage www.radioq.de wird durch das ZIV ein so genannter Stream in zwei Bandbreiten angeboten: Nutzer eines schnellen DSL-Zugangs können sich über die hervorragende Klangqualität (128 kbit/Sekunde) freuen. Für ISDN ist der Stream in abgespeckter Version (32 kbit/Sek.) verfügbar. Die zum Empfang benötigten Programme (Real Player, Windows Media Player oder Winamp) können kostenlos über die Internetseite heruntergeladen werden. Guido Wessendorf vom ZIV freut sich: „Unser leistungsfähiges Universitäts-Netzwerk mit zur Zeit über 30.000 Anschlusspunkten für Rechner, über 100 im gesamten Stadtgebiet verteilten Funk-LAN-Zellen, über 660 direkten ADSL-Verbindungen in studentische Wohnheimzimmer hinein sowie mit den über 1200 Einwahlzugängen mit den sehr günstigen *uni@home-plus*-Tarifen und natürlich dem breitbandigen Zugang zum Internet bietet die richtigen Voraussetzungen für dieses neue Angebot. Gerne haben wir Radio Q mit einem geeigneten Streamingserver unterstützt und freuen uns auf die weitere Zusammenarbeit.“

Auch Weltenbummler haben per Internet jetzt den akustischen Draht zur Studiums-Heimat. Wer in Kopenhagen, Krakau oder Kalkutta ein Auslandssemester absolviert, bleibt über Bildungspolitik, Wahlen zum Studierendenparlament und alles, was sonst in Münster passiert, auf dem Laufenden. „Im Moment zieht ja gerade das Institut für Politikwissenschaft ins Schloss um. Das kann man bei uns jetzt auch am anderen Ende der Welt hören – in gute Musik verpackt“, betont Chefredakteur Tim Karis.

Radio Q ist seit fünf Jahren das Campusradio für Münster und auch weiterhin auf „klassischem“ Weg auf 90,9 MHz und im Kabel auf 105,3 MHz zu empfangen. Der Sender bietet interessierten Studierenden die Möglichkeit, sich auszuprobieren und erste Erfahrungen im Umgang mit dem Medium Hörfunk zu erlangen.

Intro – Schließanlagen im ZIV und anderswo

E. Sturm

Studenten und Mitarbeiter können das ZIV auch außerhalb der Öffnungszeiten betreten – mit einer Schlüsselkarte, die über ein Webinterface verwaltet wird.

Seit über einem halben Jahr kann das Zentrum für Informationsverarbeitung (ZIV) in der Einsteinstr. 60 auch nachts und am Wochenende betreten werden. Studenten können auf der ZIVintro-Webseite eine Schlüsselkarte beantragen und diese danach am Service-schalter abholen. Zugelassen sind nur der Eingangsbereich, die ZIV-Pools 3 und 4 im Erdgeschoss und der Bereich der Druckausgabefächer. Ähnliches gilt für die Mitarbeiter, deren Schlüsselkarte genau die Bereiche öffnet, für die der Mitarbeiter zuständig ist. Auf diese Weise ist der mögliche Schaden bei Verlust der Karte minimiert.

Zentrales Element des Verfahrens ist die vom ZIV zugeteilte Nutzerkennung samt Passwort. Jeder, der etwas im System bewirken will, muss sich mit Kennung und Passwort ausweisen: der Student bei der Beantragung, der Kollege am Serviceschalter und auch jeder, der eine neue PIN setzen oder seine Karte sperren möchte.

Die **ZIVintro**-Webseite dient einzig und allein Studenten, die ihren Zugang zum ZIV-Pool verwalten wollen. Für Institute, die ebenfalls Studenten nachts in ihren CIP-Pool lassen wollen, ist eine eigene, zu ZIVintro analoge Webseite denkbar. Im Gegensatz dazu steht die **Intro**-Webseite, die Bediensteten der gesamten Universität bei der Verwaltung ihrer Rolle(n) in Schließsystemen der Uni unterstützt.

Zum ZIVintro-Webinterface möchte ich nur noch einmal die Abbildung aus **infoforum** Nr.2/2004 wiederholen. Auch Tipps zur Benutzung finden Sie dort.

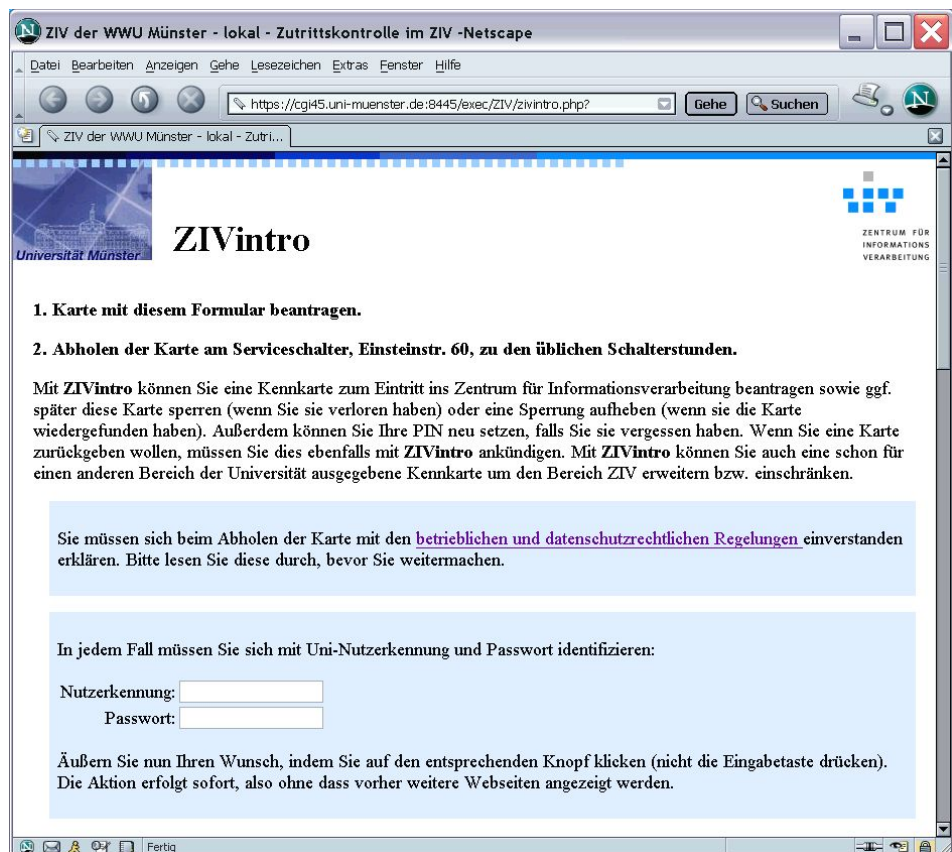


Abb. 3

Mehr soll an dieser Stelle über das (für die gesamte Uni gedachte) Intro-Webinterface gesagt werden. Grundlegend ist das Rollenkonzept: Administratoren können Rechte vergeben an andere Personen und haben selbst Rechte von anderen Administratoren verliehen bekommen. Damit die Uni-Verwaltung nicht alle Rechte für jede Person selbst eintragen muss – und das womöglich auf der Grundlage unleserlicher Briefe – werden Rechte hierarchisch vergeben, an der Spitze steht ein Uni-Supervisor. Es gibt also folgende Rollen:

Uni-Supervisor

Diese Rolle dient nur der Rechtevergabe: Der Rolleninhaber darf weitere Uni-Supervisor ernennen sowie Uni-Administratoren.

Uni-Administrator

Der Inhaber dieser Rolle macht die Arbeit: das Eintragen der Institute und Bereiche sowie das Ernennen eines jeweiligen Institutsadministrators.

Institutsadministrator

Diese Rolle dient wiederum nur der Rechtevergabe: Der Rolleninhaber darf weitere Institutsadministratoren ernennen sowie Bereichsadministratoren.

Bereichsadministrator

Der Inhaber dieser Rolle macht wiederum die Arbeit: Er trägt Mitarbeiter ein und teilt ihnen die Bereiche zu, die sie betreten dürfen.

Interessant an diesem Verfahren ist, dass z. B. ein Institutsadministrator auf seiner Webseite genau die Bereiche sieht, die der Uni-Administrator seinem Institut zugeordnet hat. Aus dieser Bereichsliste kann er mehreren Bereichsadministratoren die Bereiche zuordnen, für die diese dann Mitarbeiter „ernennen“ dürfen. Ein Bereichsadministrator sieht natürlich nur die Bereiche auf seiner Webseite, die der Institutsadministrator ihm erlaubt hat.

Für den Fall, dass das Institut auch noch Schlüsselkarten an Studenten (also nicht nur Mitarbeiter) ausgeben will, kommen noch weitere Rollen hinzu:

Sekretariat

Inhaber dieser Rolle dürfen Schlüsselkarten an Studenten ausgeben.

Operating

Operateure dürfen die Anwesenheitsliste etwa ihres CIP-Pools einsehen.

Redakteur

Ein Redakteur kann eine Erklärung bearbeiten, die von Studenten bei der Kartenausgabe unterschrieben werden muss. Außerdem kann er die Beschriftung der Schlüsselkarte entwerfen – einschließlich Logos. Die Definition erfolgt online mit Hilfe von XML.

Natürlich darf eine Person durchaus mehrere Rollen spielen. Etwa würde man einem Institutsdirektor ebenfalls die Rolle „Operating“ geben. Das kann er gleich selbst erledigen, sofern er die Rolle „Institutsadministrator“ innehat. Eine fiktive Person könnte also etwa die folgende Webseite sehen, nachdem sie Kennung und Passwort eingegeben hat:



Abb. 4

Erste Schritte zur Einführung eines Identity-Managements an der WWU

R. Mersch

Nachdem durch die Konsortiallizenz bei der Fa. IBM die Verfügbarkeit der Identity-Management-Software an den Hochschulen in NRW gesichert ist, soll nun mit der Einführung des Identity-Managements an der WWU begonnen werden. Da dies die gesamte Hochschule betrifft, sind alle Mitarbeiter(innen) zur Mithilfe aufgerufen. Es gilt, eine Bestandsaufnahme und Ideensammlung durchzuführen.

Identity-Management, eines der aktuellen Top-Themen der IT, umfasst jene Prozesse und Technologien, die der Erzeugung, Verwaltung und Benutzung von digitalen Identitäten sowie ihrer Authentifizierung und Autorisierung, dienen.

In der **info_{wwu}**-Sonderausgabe vom Dezember 2004 findet sich ein ausführlicher Artikel zu diesem Thema. Ergänzend sind folgende aktuelle Entwicklungen zu erwähnen: NRW hat eine Landeslizenz für die IBM/Tivoli-Produktpalette erworben, so dass die Verfügbarkeit der Software an den Hochschulen des Landes nun gesichert ist. Weiterhin hat die Universität Bielefeld die Erarbeitung eines Feinkonzepts in Auftrag gegeben, nachdem sie bereits im Jahre 2003 ein Grobkonzept hatte erstellen lassen. Mit der Erstellung von Grob- und Feinkonzept durch externe Dienstleister folgt Bielefeld somit dem auch von der Universität Duisburg-Essen beschrittenen Weg. Zwischen den Hochschulen des Landes wird eine weitgehende Kooperation angestrebt. Es wird uns somit möglich sein, von den für Bielefeld und Duisburg-Essen erstellten Konzepten, die in vielen, wenn auch nicht in allen, Bereichen auf unsere Universität übertragbar sein dürften, zu profitieren.

Im Bereich des ZIV soll im Jahre 2005 mit der Einführung des Identity-Managements begonnen werden, wodurch insbesondere die bisherige, etwa 15 Jahre alte Benutzerverwaltung abgelöst werden soll. Geplant ist dann eine Ausweitung des Systems auf weitere Bereiche der WWU, wofür die Vorarbeiten jetzt beginnen müssen.

Der Einsatz externer Dienstleister bedeutet für die Hochschulen Bielefeld und Duisburg-Essen zunächst einmal natürlich Kosten und eine recht hohen Einsatz eigenen Personals für dessen Begleitung und Unterstützung in der Erhebungsphase. Er bringt aber auch einen starken Impetus in das Projekt. Wenn wir eine eher evolutionäre Vorgehensweise anstreben, können wir den benötigten Schwung nur durch die gemeinsame Anstrengung der gesamten Hochschule gewinnen.

Die Anliegen dieses Artikels sind es, das Bewusstsein für diese große Aufgabe zu schaffen und eine Bestandsaufnahme und Ideensammlung zu starten. Dazu seien zunächst noch einmal die wesentlichen dem Identity Management zugrunde liegenden Konzepte skizziert (s. Abb. 5. Rollenkonzept)

Datenquellen

Personendaten werden an verschiedenen Stellen erfasst. Für Universitätsangehörige sind dies vor allem die Studierenden- und Mitarbeiter-Datenbanken HISSOS und HISSVA in der Zentralen Universitätsverwaltung. Andere Personengruppen und -daten werden von verschiedenen Universitätseinrichtungen direkt erfasst, z. B. Gastwissenschaftler von den jeweiligen Instituten, externe Bibliotheksnutzer („Bürger“) von der ULB, Konferenzteilnehmer vom Konferenzveranstalter, Mitarbeiter externer Firmen vom Auftraggeber etc. Darüber hinaus können manche Daten von den Personen selbst beigesteuert oder verändert werden.

Identity-Feed

Aus den Datenquellen müssen die Identitäten extrahiert werden. Ein Problem bilden dabei die Personen, die in mehreren Quellen auftauchen, z. B. studentische Hilfskräfte oder (weiter) studierende Mitarbeiter. Wünschenswert wäre es, die aus den verschiedenen Quellen stammenden Daten zu einer Identität zusammenzuführen, doch mag es sein, dass dies aus organisatorischen, rechtlichen oder technischen Gründen nicht möglich ist.

Dienste

Unter dem Begriff „Dienste“ sind hier die Umgebungen subsummiert, zu denen die Personen Zugang erhalten sollen. Dies umfasst weit mehr als die üblichen IT-typischen Systeme, an die man zunächst denkt. Gemeint ist hier die gesamte Spannweite von der schlichten Eintragung einer Person in ein Verzeichnis wie das Telefonbuch, über Schließsystem mit Schlüsselkarten-Vergabe, Telefonanlage, Systeme zur Veranstal-

tungs- und Prüfungsverwaltung bis hin zu Web-Access-Systemen, die den Zugang zu diversen Web-Anwendungen steuern. Dienstzugänge werden als „Accounts“ bezeichnet.

Berechtigungen

Nicht in der Abbildung dargestellt, aber ebenfalls über das Identity-Management-System gesteuert werden müssen die Rechte, die den Accounts zugeordnet sind.

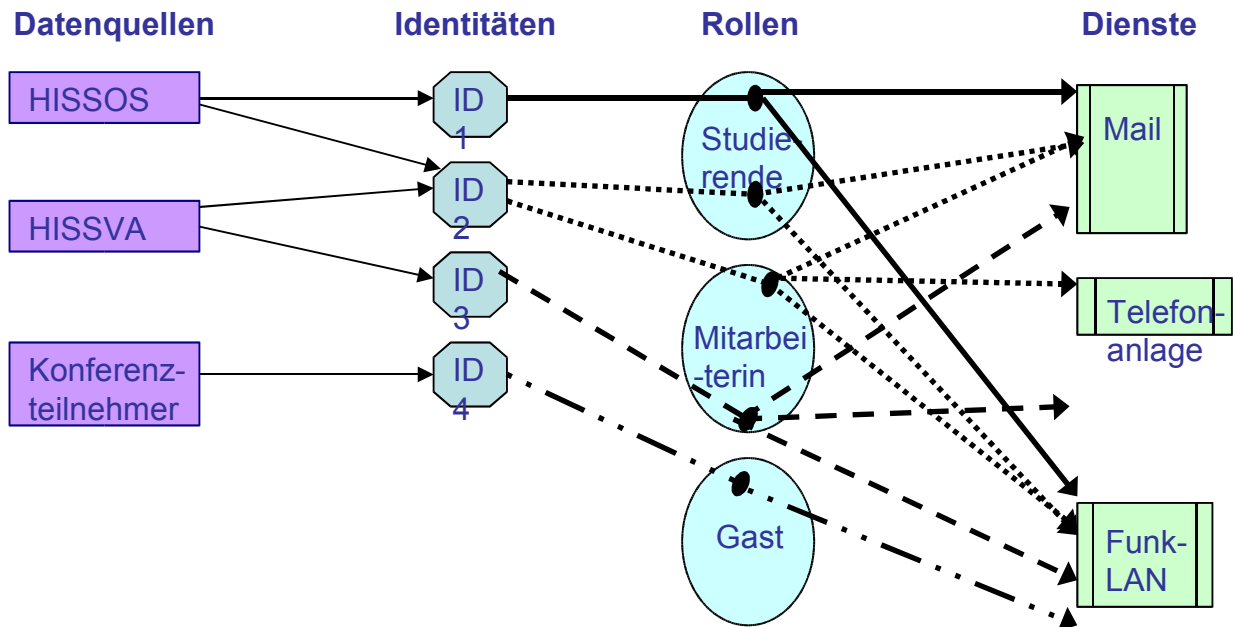


Abb. 5. Rollenkonzept

Rollen

An zentraler Stelle im Identity-Management befindet sich das Rollenkonzept, über das gesteuert wird, welche Accounts und Berechtigungen einer Person zugeordnet werden. Dazu werden den Identitäten, möglichst automatisch auf der Basis der aus den Datenquellen stammenden Informationen, die Rollen zugeordnet, die diese Person in der Universität innehat. Eine Person kann mehrere Rollen haben. Um die Vergabe von Accounts und Berechtigungen möglichst genau steuern zu können, erscheint ein fein gegliedertes Rollenkonzept wünschenswert, andererseits ist es aus Gründen der Übersichtlichkeit vorteilhaft, sich auf eine eher geringe Anzahl von Rollen zu beschränken. Hier muss ein vernünftiger Mittelweg gefunden werden.

Aufruf zur Bestandsaufnahme und Ideensammlung

Die Informationen, die für die Konzeptionierung eines Identity-Management-Systems aus den verschiedenen Bereichen der Universität benötigt werden, sind:

- Welche Datenquellen gibt es außer den genannten? Wo also werden zurzeit oder künftig Personendaten erfasst?
- Welche Rollen sollten bedacht werden? Eine Rolle ist insbesondere dann zu berücksichtigen, wenn sich aus ihr ein spezielles Zugangsmuster zu den diversen Diensten ergibt.
- Welche Dienste sollen in das System aufgenommen werden? An dieser Stelle ist es durchaus angebracht, mal quer, und über den durch den IT-Bereich gesteckten Horizont hinaus, zu denken.

- Welche Prozesse und Abläufe gibt es oder sind geplant?

Die Antworten auf diese Fragen sollten an die jeweiligen IVVen gemeldet werden, die diese für ihre Bereiche bitte sammeln und koordinieren.

Zur Sonderausgabe **infoforum**

E. Sturm

Eine Zusammenstellung der Themen unserer **infoforum**-Sonderausgabe

Zum 40-jährigen Bestehen des ZIV, zum 20-jährigen Bestehen des Universitäts-LAN und zum 20-jährigen Bestehen des Computer-Investitions-Programms (CIP) hat das ZIV eine Sonderausgabe des **infoforum** herausgegeben, die ungefähr gleichzeitig mit dieser regulären Ausgabe verteilt wird. Um auch den Lesern, die kein Exemplar der Sondernummer bekommen haben, einen Einblick zu vermitteln und vielleicht dazu zu motivieren, sich einzelne Artikel im Web anzuschauen, bringen wir hier eine kommentierte Zusammenfassung der Artikel:

Grußworte

Folgende Autoren haben Grußworte im weitesten Sinne zu den oben genannten Jubiläen an das ZIV gerichtet – Betrachtungen zu Vergangenheit, Gegenwart und Zukunft (in alphabetischer Reihenfolge der Nachnamen):

Dr. L. Becker (Sprecher der IVV-Leiter):

Grußwort der IVV-Leiter

Prof. Chr. Bischof, Ph. D. (Sprecher des Arbeitskreises der Rechenzentrumsleiter NRW (ARNW), Leiter des Rechen- und Kommunikationszentrums und Inhaber des Lehrstuhls für Hochleistungsrechnen der RWTH Aachen):

Hochschulübergreifende IT-Kommunikation und der Ressourcenverbund NRW (RV-NRW)

Dr. B. Böhm (Kanzlerin), Dr. W. Held (Direktor des ZIV), Dr. B. Tröger (Direktorin der ULB):

IKM-Service – eine erste Bilanz

Dr. W. A. Brett (Ministerium für Wissenschaft und Forschung des Landes Nordrhein-Westfalen):

20 Jahre LAN, 20 Jahre CIP und 40 Jahre ZIV – und was kommt dann? Betrachtungen zur Weiterentwicklung im IuK-Bereich

Prof. Dr. W. Griebhaber (Vorsitzender des IV-Lenkungsausschusses):

Grußwort des IV-Lenkungsausschusses

Prof. Dr. H. L. Grob (Institut für Wirtschaftsinformatik, Universität Münster):

Wissensnetzwerke in der cHL-Architektur

Prof. Dr. W.-M. Lippe (Institut für Angewandte Informatik an der und geschäftsführender Direktor des Instituts für Informatik der WWU):

Institut für Angewandte Informatik und ZIV – eine jahrelange erfolgreiche Zusammenarbeit

Dipl.-Phys. K. Reichel (Vorsitzender des Personalrats der wiss. Beschäftigten):

Grußwort des Personalrats der wiss. Beschäftigten

Dipl.-Ing. H. Schlattmann (Leiter der Datenverarbeitungszentrale), Chr. Hachtkemper (Leiter Hochschulkommunikation Fachhochschule Münster):

Kooperation heißt das Konzept

Prof. Dr. J. Schmidt (Rektor der Universität Münster):

Grußwort des Rektors

K. Ullmann (DFN-Verein):

Zum 40jährigen Jubiläum des ZIV

ZIV-Aktuell

Prof. Dr. Dr. h. c. M. Wasna (ehemalige Rektorin der WWU und Vorsitzende des Fördervereins Baltikum e. V.):

Förderung der Universitäten in den Baltischen Staaten

Prof. Dr. G. Vossen (Wirtschaftsinformatik, Universität Münster, Vizepräsident der Gesellschaft für Informatik):

Rechenzentren: noch wandelbar in diesen Zeiten?

Dr. W. Zierau (Vorsitzender der IV-Kommission):

Grußwort des Vorsitzenden des IV-Kommission

Die Jubiläen

Aus dem eigenen Hause stammen die folgenden Artikel, die auf die einzelnen Jubiläen speziell eingehen (ab hier verzichten wir – wie im **infoforum** üblich – auf die persönlichen Titel der hauseigenen Autoren):

W. Held, W. Bosse:

Editorial

W. Bosse:

Gelebter Wandel: 40 Jahre Rechenzentrum

W. Held:

Die IV-Versorgung der Universität – ein Erfolgsmodell

W. Lange, O. Winkelmann:

Zwanzig Jahre CIP

G. Richter:

Zwanzig Jahre LAN

Aus dem ZIV

Die folgenden Artikel beleuchten spezielle Aspekte des ZIV:

W. Bosse:

IV-Kompetenz erwerben!

W. Held:

Kosten – Die andere Seite der Leistungen

W. Kaspar:

Schnelle Hilfe bei IV-Problemen

Rechnernetz

Speziell mit dem Rechnernetz der Universität beschäftigen sich die folgenden Artikel:

A. Forsmann:

Mit dem Notebook ins Rechnernetz

M. Kamp:

Die Netzdatenbank des ZIV

M. Speer:

Entwicklung des Netzwerkmanagements

G. Wessendorf:

Technische Evolution im Netz

Sicherheit

Das Thema der folgenden Artikel ist Sicherheit – sowohl auf den Rechnern, als auch für die Gebäude:

W. Held, St. Ost, G. Richter:

Sicherheit der IV – ein endloses Thema

Dr. U. Helmbrecht (Präsident des BSI):
Förderung der IT-Sicherheit an Hochschulen

E. Sturm:
Administration elektronischer Schließanlagen der Institute

E. Sturm:
Die Schließanlage im ZIV

System-Management

Bei den folgenden Artikeln geht es um Betriebssysteme und deren Verwaltung:

M. Grote:
Systemüberwachung

J. Hölters:
Abrechnung von IV-Diensten

M. Leweling:
Hochleistungsrechnen – der Linux-Parallelrechner oder wie bekommt man 100 Jahre Rechenzeit in 18 Monaten?

R. Mersch:
10 Jahre Backup und Archivierung

R. Mersch:
Identity Management – geordneter Zugang zu Ressourcen und Informationen

St. Ost:
MARIONet: Eine moderne System-Management-Struktur

Th. Bauer, H.-H. Adam, B. Baumeier, W. Zierau:
MORFEUS: Ungenutzte Arbeitsplatzrechner als Rechenfarm für wissenschaftliche Anwendungen

Anwendungen

Auch Anwendungen nahmen immer einen großen Raum ein, wie die folgenden Artikel zeigen:

H. Kamp:
Blindenarbeit und Computer: Seit fast 40 Jahren eine Erfolgsstory

H. Kamp:
Ein gewichtiges Buch

H. Kamp:
Modernste Methoden der Frühmittelalterforschung

W. Kaspar:
TeX an der WWU

H.-W. Kisker, A. Scheffer:
Multimedia im ZIV

B. Süselbeck:
Softwareverteilung – Evolution und Revolution

Internet

Selbstverständlich beschäftigen wir uns auch mit dem Internet:

W. Kaspar:
Zum Internet-Auftritt unserer Universität

B. Neukäter:
Publizieren im Internet

R. Perske:
perMail

A. Stolze:
JOIN

Leider stand bis Redaktionsschluss dieser Ausgabe des **info^{rum}** die exakte Webadresse der Sonderausgabe noch nicht fest, sodass ich hier nur auf die Leitseite des ZIV verweisen kann: <http://www.uni-muenster.de/ZIV/>.

Neues von perMail

R. Perske

perMail wurde wieder um zahlreiche neue Möglichkeiten ergänzt, dieser Artikel gibt einen kurzen Überblick.

Seit dem letzten Artikel über perMail im **info^{rum}** Nr. 3/2003 hat es wieder zahlreiche kleine und große Verbesserungen und Erweiterungen gegeben. Das meiste hat sich dabei unsichtbar für den Nutzer unter der Oberfläche getan, um die vollständige Internationalisierung in der zukünftigen Version 2.0 vorzubereiten. Sichtbares Zwischenergebnis ist die Darstellung nicht nur des Textes, sondern auch der Betreff- und Adresszeilen in beliebigen Zeichensätzen.

Auffälligste Neuerung ist die trainierbare Spam-Erkennung, welche ganz ähnlich funktioniert wie die Software Deleatur meines Kollegen E. Sturm. Diese Spam-Erkennung beschreibe ich ausführlich im folgenden Artikel.

Es gibt aber auch kleinere Erweiterungen, die ich Ihnen in kurzen Worten beschreiben darf:

- Schon seit Anfang des Jahres können auch die Nutzer derjenigen WWW-Programme mehr als eine Anlage gleichzeitig an eine E-Mail hängen, die grundlos bei Datei-Eingabefeldern die Angabe nur einer Datei erlauben: Ab der Bedienoberfläche Text gibt es auf der Neue-E-Mail-Seite jetzt zehn Datei-Eingabefelder.
- Es gibt jetzt die Möglichkeit, schon in der WWW-Adresse der perMail-Login-Seite einige oder alle Eingabefelder außer dem Passwort in Form eines „Query-String“ anzugeben. Dies ist insbesondere sinnvoll, wenn man sich ein Lesezeichen (Bookmark) auf die Login-Seite einrichtet. Beispielsweise stellt folgende WWW-Adresse die Nutzerkennung „perske“ (`user=perske`), die englische Sprache (`lang=en`), und „Beginne mit ... Wegsortieren“ (`init=f`) ein:

`https://permail.uni-muenster.de?user=perske&lang=en&init=F`

Mögliche Angaben bei „init=“ sind: I (Index), N (Neue E-Mail), A (Adressbuch), K (Kalender), F (Wegsortieren), S (SPAMfilter), R (Reparieren), O (Einstellungen).

- Ähnlich wie im Unix- und PC-E-Mail-Programm „pine“ enthält auch perMail jetzt eine Zoom-Funktion. Falls Sie einen Teil Ihrer E-Mail markiert haben, können Sie über das Auswahlfeld „Sichtbar“ unten auf der Index-Seite auswählen, ob nur die markierten, nur die unmarkierten oder alle E-Mails aufgelistet werden. Insbesondere im Zusammenspiel mit der Suchfunktion hilft die Zoom-Funktion, den Überblick zu behalten.
- Zwar handelt es sich beim Eingabefeld für den Text einer neuen E-Mail prinzipbedingt nur um ein einfaches Eingabefenster, doch besitzt perMail jetzt gewisse Fähigkeiten, um den Text ansprechend zu formatieren. Dies gilt bereits, wenn beim Antworten die Original-E-Mail zitiert wird – übrigens werden jetzt auch Texte aus reinen HTML-E-Mails zitiert –, insbesondere aber auch bei Benutzung der Schaltfläche „Text ausrichten“.

Dann bemüht perMail sich, Absätze mit ordentlichen und sinnvollen Zeilenumbrüchen zu versehen; es weiß auch mit Zitaten und E-Mail-Kopfzeilen sinnvoll umzugehen und kann sogar Aufzählungslisten ordentlich formatieren.

Wie jede Pseudointelligenz bei Computern rät natürlich auch perMail nicht immer richtig, was Sie eigentlich möchten; daher sollten Sie beim Eintippen Ihres Textes zwischen zwei Absätzen immer eine Leerzeile einfügen. Absätze, die Sie mit einem einzelnen Bindestrich, Sternchen o. Ä. oder mit einer Aufzählungsnummer oder einem Aufzählungsbuchstaben (mit Punkt oder rechter Klammer) anfangen, werden als Elemente einer Aufzählungsliste erkannt, deren Folgezeilen eingerückt werden.

- Es gibt einen kleinen Terminkalender, der sogar mit regelmäßigen Terminwiederholungen („jeder vorletzte Mittwoch im ungeraden Monat“ usw.) umgehen kann. Sobald Sie dort Termine eingetragen haben, wird auf jeder Seite rechts oben unter dem Datum der jeweils nächste Termin in Form eines Auswahlfeldes eingeblendet. Durch Aufklappen können Sie dann auch die vorherigen und nächsten Termine sehen.
- Alle Symbole gibt es jetzt auch in einer mittleren Größe.
- Anzahl und Leistungsfähigkeit der perMail-Server wurden der steigenden Nutzung angepasst.

Einen umfassenden Überblick über sichtbare Änderungen zwischen den Versionen finden Sie immer in der Online-Hilfe unter

<http://permail.uni-muenster.de/help-de-changes.html>.

Spam-Entsorgung mit perMail

R. Perske


perMail besitzt jetzt eine trainierbare Spam-Erkennung. Bei geschickter Nutzung lassen sich Spam-E-Mails effizient vernichten.


perMail integriert verschiedene Methoden, um unerwünschte E-Mails aus dem eigenen Postfach auszusortieren. Dieser Artikel beschreibt, welche Ansätze in perMail integriert sind, und liefert eine ausführliche Anleitung, wie Sie durch geschickte Kombination der in perMail enthaltenen Möglichkeiten dem unerwünschten Werbemüll effizient zu Leibe rücken können – sofern Sie bereit sind, die für das Training notwendige Zeit zu investieren.

Regelbasierte Spam-Erkennung

Ein erster Ansatz beruht auf der Erkenntnis, dass sich viele Spam-E-Mails anhand typischer technischer Eigenschaften, beispielsweise bestimmter Muster in den Kopfzeilen, erkennen lassen.

Auf den zentralen E-Mail-Servern der Universität ist die Software SpamAssassin installiert, welche alle durchlaufenden E-Mails auf bekannte solche Eigenschaften hin untersucht, und bei verdächtigen E-Mails zusätzliche Kopfzeilen mit dem Ergebnis der Untersuchung einfügt. Unter anderem summiert SpamAssassin die Ergebnisse der verschiedenen Tests zu einer Gesamtanzahl von Spam-Punkten auf – die Anzahl der Sternchen in der eingefügten Kopfzeile „X-Spam-Level: *****“ entspricht dieser Punktzahl – und vergibt oberhalb einer Grenzpunktzahl die zusätzliche Kopfzeile „X-Spam-Flag: YES“.

 3.7

 9.2



perMail zeigt die von SpamAssassin vergebenen Spam-Punkte an. Auf der Index-Seite finden Sie die Anzeige in der rechten Spalte mit der Überschrift „SPAM“, auf der Ansicht-Seite in der Überschriftenzeile rechts. Bei vorhandener Zeile „X-Spam-Flag: YES“ ändert sich das Symbol, siehe Abbildungen im Rand.

perMail bietet Ihnen eine Schaltfläche „SPAMfilter“. Dieser SPAMfilter sorgt im Posteingang dafür, dass alle E-Mails mit „X-Spam-Flag: YES“ sofort aus dem Posteingang im elektronischen Reißwolf verschwinden. Die nur als verdächtig eingestuften E-Mails bleiben im Posteingang. Auch bei der Anmeldung können Sie schon „Beginne mit ... SPAMfilter“ auswählen (und durch „init=s“ im „Query-String“ sogar schon im Lesezeichen einstellen, siehe vorherigen Artikel).

perMail bietet Ihnen weiterhin eine Schaltfläche „Wegsortieren“. Die dadurch ausgelösten Ablage-Aktionen können Sie durch Einrichtung entsprechender Wegsortierregeln frei programmieren. Die voreingestellten Wegsortierregeln sorgen im Posteingang dafür,

dass alle E-Mails mit „X-Spam-Flag: YES“ in die Abfalltonne geworfen werden und dass alle weiteren E-Mails mit mindestens fünf Spam-Punkten in einem Ordner „spam-messages“ abgelegt werden. Dahinter steckt die Idee, verdächtige E-Mails erst einmal beiseite zu legen und zu einem späteren Zeitpunkt noch einmal nachzuschauen, ob sich nicht doch eine erwünschte E-Mail darunter befindet. Wer diese Wegsortierregeln benutzt, sollte also alle paar Tage mal den Inhalt des Ordners „spam-messages“ sichten und anschließend vernichten.

Natürlich bemühen sich die Spam-Versender, ihre Massen-E-Mails so zu gestalten, dass sie von bekannter Anti-Spam-Software wie SpamAssassin nur schlecht erkannt werden können; daher ist die Erkennungsrate nur mit Hilfe dieser Spam-Punkte nur mäßig gut. Ein bedeutender Anteil Spam-E-Mails wird nicht als Spam erkannt werden. Diesem Nachteil gegenüber steht der Vorteil, dass Sie die soeben beschriebenen Möglichkeiten sofort und ohne vorbereitende Arbeiten nutzen können.

Trainierte Spam-Erkennung

Ein zweiter Ansatz beruht auf der Erkenntnis, dass sich die meisten Spam-E-Mails daran erkennen lassen, dass sich ihr Wortschatz von dem Wortschatz erwünschter E-Mails unterscheidet. Dieser Ansatz hat das grundsätzliche Problem, dass sich beide Wortschätze nicht anhand fester Kriterien voneinander unterscheiden lassen und sich auch im Laufe der Zeit ändern. Insbesondere hängt der Wortschatz erwünschter E-Mails sehr von der Person des Empfängers ab. Die Unterscheidung muss also anhand statistischer Kriterien oder künstlicher Intelligenz erfolgen. Diesen Ansatz verfolgen viele Software-Produkte mit so genannten Bayes-Filtern und auch die im [infoforum](#) schon früher beschriebene Software „Deleatur“ meines Kollegen E. Sturm.

All dieser Software gemeinsam ist, dass man sie erst trainieren muss, bevor man sie benutzen kann. Die Software muss lernen, welche Wörter eher in Spam-E-Mails vorkommen und welche eher in erwünschten E-Mails. Man muss der Software also sowohl zahlreiche Spam-E-Mails als auch zahlreiche erwünschte E-Mails vorlegen und ihr jeweils mitteilen, zu welcher Kategorie die jeweiligen E-Mails gehören. Je umfangreicher die Software trainiert wird, desto besser wird die Spam-Erkennung.

00%g
69%S
94%O

Auch die neue trainierbare Spam-Erkennung von perMail funktioniert nach diesem Prinzip: Für jedes Wort wird gezählt, wie häufig es in Spam-E-Mails und wie häufig es in erwünschten E-Mails vorkommt. Bei der Ermittlung der Wörter wird auf Spam-typische Verschleierungstaktiken wie das Einstreuen von Satzzeichen oder Akzenten Rücksicht genommen. Mit Hilfe der durch das Training angelegten Wortbasis berechnet perMail für jede E-Mail anhand der darin enthaltenen Wörter eine Spam-Wahrscheinlichkeit zwischen 0 % und 99 % und zeigt diese ebenfalls an den oben genannten Stellen an. Zusätzlich gibt ein Buchstabe an, ob die E-Mail bereits als „gute“ (g) oder Spam- (s) E-Mail „klassifiziert“ wurde oder ob dies noch offen (o) ist.

Natürlich hängt der Wert der Aussage, eine E-Mail habe 70 % Spamwahrscheinlichkeit, sehr vom Umfang des Trainings und der dadurch aufgebauten Wortbasis ab.

Einmalige Vorbereitung: Die Wegsortierregeln

Meine persönlichen Erfahrungen lassen die folgenden Kriterien nach ausreichendem Training als sehr brauchbar erscheinen:

1. Wenn eine E-Mail schon von SpamAssassin sicher als Spam eingestuft wurde, ist sie sicher Spam.
2. Wenn für eine E-Mail von perMail eine Spam-Wahrscheinlichkeit von mindestens 75 % errechnet wurde, ist sie sicher Spam.
3. Wenn die beiden folgenden Bedingungen zusammentreffen, ist die E-Mail ebenfalls sicher Spam.
4. Wenn eine E-Mail von SpamAssassin mindestens 4 Punkte erhalten hat, ist sie sehr wahrscheinlich Spam.

5. Wenn für eine E-Mail von perMail eine Spam-Wahrscheinlichkeit von mindestens 60 % errechnet wurde, sind sehr wahrscheinlich Spam.



Diese Bedingungen lassen sich einfach in Regeln übersetzen, die auf der Wegsortierregel-Seite von perMail eingetippt werden können:

```
#1. E-Mails mit X-Spam-Flag: YES aus Posteingang in spam-archiv
field      = X-Spam-Flag
current    =
condition  = contains
data       = YES
folder     = spam-archiv

#2. E-Mails mit 75 % aus Posteingang in spam-archiv
field      =
current    =
condition  = exists
spampercent >= 75
folder     = spam-archiv

#3. E-Mails mit 4 Sternen und 60 % aus Posteingang in spam-archiv
field      = X-Spam-Level
current    =
condition  = contains
data       = ****
spampercent >= 60
folder     = spam-archiv

#4. E-Mails mit 4 Sternen aus Posteingang in spam-verdacht
field      = X-Spam-Level
current    =
condition  = contains
data       = ****
folder     = spam-verdacht

#5. E-Mails mit 60 % aus Posteingang in spam-verdacht
field      =
current    =
condition  = exists
spampercent >= 60
folder     = spam-verdacht
```

Diese fünf Regeln entsprechen den fünf oben genannten Kriterien und wirken durch die Angabe „current“ nur im Posteingang. Sicher erkannte Spam-E-Mails landen damit im Ordner „spam-archiv“, wo sie für ein späteres weiteres Training zur Verfügung stehen. Als Spam-verdächtig erkannte E-Mails landen im Ordner „spam-verdacht“, der regelmäßig gesichtet werden sollte.

Zwei weitere Regeln ersparen beim Training und im weiter unten beschriebenen Tagesgeschäft einige Mausklicks:

```
#6. Alle E-Mails aus Ordner spam-verdacht in Ordner spam-archiv
field      =
current    = spam-verdacht
condition  = exists
folder     = spam-archiv

#7. Alle E-Mails aus Ordner spam-archiv in den Reißwolf
field      =
current    = spam-archiv
condition  = exists
folder     = /
```

Die sieben Regeln machen erst dann einen Sinn, wenn bereits ein ausreichendes Training durchgeführt wurde – jeweils mehr als hundert gute und Spam-E-Mails sollten es schon gewesen sein –, daher sind diese Wegsortierregeln nicht voreingestellt, sondern müssen von Ihnen selbst aktiviert werden.

Natürlich können diese Regeln von Ihnen nach Belieben ergänzt oder geändert werden; Whitelists oder Blacklists sind einfach zu erstellen. In der Online-Hilfe finden Sie ein umfangreiches, kürzlich erneuertes Beispiel von Wegsortierregeln, in welchem die obigen Regeln als Kern enthalten sind und welches eine komplette Beschreibung der Syntax dieser Regeln enthält:

<http://permail.uni-muenster.de/help-filterrules.txt>

Ohne Fleiß kein Preis: Das Training



Wenn Sie sich auf der Index-Seite und der Ansicht-Seite genauer umschauen, werden Sie an verschiedenen Stellen die Schaltflächen „Als Nicht-SPAM klassifizieren“ und „Als SPAM klassifizieren“ finden, die entsprechenden Symbole sind im Rand abgebildet. Die Schaltflächen dienen zum Klassifizieren der E-Mails und somit zum Training: Sie teilen perMail damit mit, dass Sie die jeweiligen E-Mails als erwünschte oder als Spam-E-Mails betrachten.

Natürlich wäre es jetzt unerträglich mühsam, beim Durchblättern Ihrer E-Mails immer wieder nacheinander auf „Als ... klassifizieren“ und auf „Nächste E-Mail“ zu klicken, insbesondere da das Klassifizieren einen kleinen Moment dauert. Daher empfiehlt sich folgende Vorgehensweise:

Arbeiten Sie mit Ihren E-Mails, wie Sie es gewohnt sind, ohne sich um das Training zu kümmern, aber beachten Sie folgende beiden Punkte:



- Werfen Sie Spam-E-Mails nicht sofort weg, sondern sammeln Sie sie in einem eigenen Ordner, beispielsweise „spam-archiv“.



- Benutzen Sie für erwünschte, aber nicht mehr benötigte E-Mails nicht den Reißwolf, sondern die Abfalltonne, und verzichten Sie vorerst darauf, die Abfalltonne zu leeren.

Alle paar Tage oder Wochen, je nach Terminplan und freiem Plattenplatz, führen Sie dann eine Trainingssitzung durch:



- Gehen Sie in den Ordner „spam-archiv“ und klicken Sie unten auf der Index-Seite auf „Alle E-Mails als SPAM klassifizieren“. Das dauert etwas, aber danach können Sie auf „Alle E-Mails wegsortieren“ klicken. Obige 7. Regel vernichtet dann den gesamten Inhalt des Ordners und erspart Ihnen, erst noch alle E-Mails zu markieren.
- Gehen Sie nacheinander in die Abfalltonne und in die anderen Ordner, in denen Sie in letzter Zeit E-Mails abgelegt haben, und klicken Sie jeweils auf „Alle E-Mails als Nicht-SPAM klassifizieren“. Zu diesen anderen Ordnern gehört natürlich auch die Standardablage, in der die Kopien der von Ihnen abgeschickten E-Mails abgelegt werden. Danach können Sie auch die Abfalltonne leeren.

Die Trainingssitzung kostet Sie jetzt zwar einige Minuten, nimmt aber weit weniger Zeit in Anspruch als wenn Sie jede E-Mail einzeln klassifizieren würden.

perMail merkt sich für eine gewisse Zeit, welche E-Mails Sie bereits klassifiziert haben, und vermeidet so doppeltes Klassifizieren.

Tagesgeschäft: Aussortieren von Spam



Obige Wegsortierregeln machen Ihnen das Aussortieren der Spam-E-Mails sehr einfach: Klicken Sie einfach im Posteingang unten auf der Index-Seite auf „Alle E-Mails wegsortieren“. Sie können sogar schon bei der Anmeldung „Beginne mit ... Wegsortieren“ auswählen (und dies durch „init=f“ im „Query-String“ sogar schon im Lesezeichen einstellen, siehe vorherigen Artikel). Die ersten fünf Regeln erledigen dann den Rest.

Mit den übrig bleibenden E-Mails arbeiten Sie dann wie gewohnt und oben beschrieben weiter. Natürlich werden immer wieder auch Spam-E-Mails übrig bleiben, diese sollten

Sie weiterhin in „spam-archiv“ ablegen, damit perMail diese beim nächsten Training zu sehen bekommt.

Das war es eigentlich schon, aber alle paar Tage sollten Sie einen Blick in den Ordner „spam-verdacht“ werfen und nachschauen, ob vielleicht doch eine erwünschte E-Mail den Weg dorthin gefunden hat. Solche E-Mails sollten Sie dann zurück in den Posteingang ablegen. Danach können Sie in diesem Ordner auf „Alle E-Mails wegsortieren“ klicken. Obige 6. Regel legt dann den gesamten Inhalt des Ordners in „spam-archiv“ ab und erspart Ihnen somit, erst noch alle E-Mails zu markieren und den Ablageordner herauszusuchen.

Falls Sie keine Lust haben, regelmäßig in diesen Spam-Verdacht-Ordner zu schauen, dafür aber bereit sind, ein paar mehr Spam-E-Mails in Ihrem Posteingang vorzufinden und händisch abzulegen, können Sie oben einfach die Wegsortierregeln 4, 5 und 6 weglassen. Dann bleiben auch die nur als wahrscheinlich Spam eingestuft E-Mails im Posteingang.

Etwas Statistik

Wichtig ist mir besonders, dass keine E-Mail zu Unrecht aussortiert wird; dementsprechend vorsichtig sind die oben genannten Kriterien gewählt. Die von mir nach längerer Nutzung gemessene Erkennungsquote von 95 % bei einer False-Positive-Quote von Null ist sicherlich ein gutes Ergebnis.

Weitere 3 % landen in meinem Verdacht-Ordner (leider auch etwa eine echte E-Mail im Monat); nur 2 % verbleiben unerkannt im Posteingang. Bei einem Verzicht auf den Spam-Verdacht-Ordner würden also 5 % aller Spam-Mails im Posteingang verbleiben.

Warum kein zentrales Training?

Warum übernimmt nicht das ZIV die Mühe, eine solche Spam-Erkennung zentral zu trainieren, die dann so wie SpamAssassin Markierungen im Kopf einfügt? Dann bräuchten die einzelnen Nutzer in ihren E-Mail-Programmen doch nur noch einen Schalter umzulegen, um die markierten E-Mails automatisch wegzuworfen, werden viele Leser denken.

Leider hat jedoch das Training die Eigenschaft, eine individuell auf den oder die Trainierenden zugeschnittene Spam-Erkennung zu erzeugen, welche leider nicht für die Allgemeinheit brauchbar ist. Das gilt selbst dann, wenn eine größere Gruppe von ZIV-Mitarbeitern mit allen ihren E-Mails an diesem Training teilnehmen würden – ein solchermaßen trainierter Filter wäre nur für ZIV-Mitarbeiter brauchbar.

Einige Beispiele verdeutlichen das: Wenn ein ZIV-Mitarbeiter E-Mails mit chinesischen Schriftzeichen erhält, handelt es sich praktisch immer um Spam. Die Software würde lernen, chinesische Texte immer als Spam zu bewerten. Die Mitarbeiter des Instituts für Sinologie und Ostasienkunde würden es aber überhaupt nicht lustig finden, wenn ein Großteil ihrer Korrespondenz als Spam gebrandmarkt würde. Genausowenig sollten sachliche Diskussionen von Pharmazeuten und Medizinern über lebensgefährliche Nebenwirkungen potenzsteigernder Mittel oder von Wirtschaftsfachleuten über Anlageformen und Renditen als Spam gewertet werden, nur weil uns ZIV-Mitarbeitern Reizwörter wie Mortgage, Payment, Investment, Viagra usw. nur in Spam-E-Mails begegnen. „Universität“ und „universell“ haben nicht ohne Grund den gleichen Wortstamm. Daher macht es keinen Sinn, die durchaus vorhandenen entsprechenden Komponenten der Software SpamAssassin auf den zentralen Mailservern zu aktivieren.

Das heißt also, dass Ihnen die Mühe des individuellen Trainierens nicht erspart bleibt, falls Sie Deleatur, die trainierbare Spam-Erkennung von perMail oder eine andere auf diesem Ansatz beruhende Software einsetzen möchten und eine wirklich gute Spam-Erkennung erreichen möchten.

Fazit

Betroffen durch mittlerweile über 350 Spam-E-Mails pro Tag habe ich die trainierbare Spam-Erkennung in perMail und die in diesem Artikel beschriebene Vorgehensweise

vor allem zu meiner eigenen Entlastung entwickelt, aber auch zur Integration von Deleatur in perMail. Allen perMail-Nutzern steht daher jetzt eine Methode zur Verfügung, effizient und ohne Zusatzprogramme auch größere Spam-Fluten zu entsorgen.

AutoDeleatur

E. Sturm

Deleatur 1.9.3 bringt ein weiteres Szenarium: Automatisch schaut das Programm alle 20 Minuten nach Mail und löscht Spam.

Wer schaut schon alle 20 Minuten nach Mail? Nach Stunden hat sich dann aber wieder so viel angesammelt, dass das Prüfen auf Spam lästig wird. Deleatur-Benutzer verwenden zwar Deleatur zum Nachschauen und starten ihr eigenes Mailprogramm nur, wenn ordentliche Mail übrig geblieben ist. Aber auch dann muss man mehrfach die Eingabetaste drücken, bis alles vorbeigerauscht ist.

Die neue Version 1.9.3 erlaubt die Angabe des Parameters e , der angibt, alle wie viel Minuten Deleatur automatisch nach Mail schauen soll. Man könnte etwa in der Datei `deleatur.prm` folgende Zeilen hinzufügen:

```
r=0
z=0
e=20
o=10000
u=5000
l=80
a=10
```

Dann kommen auch keine Rückfragen, ob eine Mail Spam ist ($r=0$), und auch nicht am Ende des Fensters, ob weitergeblättert werden soll ($z=0$). Ist der Parameter e angegeben, so wird auch ggf. die Wortbasis ohne zu fragen reduziert, und zwar wenn die Obergrenze (hier etwa 10 MB) erreicht ist, auf höchstens den Untergrenzwert (hier etwa 5 MB). Wer eine Eselsbrücke braucht: Wenn man e angibt, läuft das Programm ewig.

In dieser Einstellung löscht Deleatur alles, was über 80 % Spamwahrscheinlichkeit ($l=80$) besitzt und akzeptiert alles unter 10 % ($a=10$). Die Wörter dieser Mails werden auch gelernt. Alle anderen Mails sind noch nicht in die Wortbasis eingegangen.

Wie ist also nun das Szenarium? Um nach Mail zu schauen, braucht man jetzt nur nachzuschauen, ob im Deleaturfenster etwas angezeigt wird. Ist das der Fall und gibt es Mails, deren Charakter noch nicht festgelegt wurde, so sollte man eine normal parametrisierte Version von Deleatur starten und die unentschiedenen Mails bewerten.

Ist dann noch etwas Gutes übrig geblieben, so starte man sein übliches Mailprogramm, sei es PerMail, Netscape, Outlook Express oder Pine. Natürlicherweise ist man in diesem Szenarium 20 Minuten hinter der Zeit, aber wen stört das schon?

Die neue Version von Deleatur kann wie üblich von ZIVsoft heruntergeladen werden (<https://www.uni-muenster.de/zivsoft/>).

Neues zum SPSS

S. Zörkendörfer

Auch ein Jubiläum: Nach 9 Versionen SPSS und 3 Versionen SPSSX am Großrechner und 12 Versionen SPSS am PC wird nun eine 25. Version erwartet.

Für den Landeslizenzvertrag zum Statistik-Paket SPSS begann am 1. Dezember ein neues Lizenzjahr, Informationen hierzu können Sie u. a. auf der Webseite www.uni-muenster.de/ZIV/Organisation/SoftwareVerteilungSPSS.html einsehen. Der Lizenzvertrag lässt auch eine (allerdings kostenpflichtige) Weitergabe zur Nutzung am häuslichen Arbeitsplatz zu. Die meisten „Abonnenten“ werden rechtzeitig eine Bestellung für die neue Lizenzperiode eingereicht haben und mit den neuen Lizenzcodes versorgt sein, und zwar standardgemäß für die Produkte SPSS 12 deutsch, AMOS 5.0, AnswerTree 3.1 deutsch, DataEntry Builder 4, Axum 7 auf einer Windows-Workstation. Abweichend hiervon können wir berechnete Nutzer auf Zuruf mit Zugängen zu SPSS 12 englisch, SPSS 11 deutsch oder englisch, AnswerTree 3.1 englisch unter Windows so-

wie SPSS 10 und 11 unter MacOS versorgen. Ein Versionswechsel muss nicht notwendig zum Beginn des Lizenzjahres erfolgen.

Im Laufe des Lizenzjahres dürfen wir mit der Auslieferung einer Version 13 rechnen. Bezüglich SPSS 13 finden sich aktuelle Ankündigungen zur Änderung der Autorisierung (Lizenzcodes) sowohl auf den Internet-Seiten der Muttergesellschaft (www.spss.com) wie der deutschen SPSS GmbH, und damit verbunden wurde landesweit bereits aufgeregt berichtet. Wir werden diesbezüglich erst dann berichten und Stellung beziehen, wenn für unsere Lizenzvereinbarung zutreffende konkrete Angebote oder Regelungen formuliert worden sind. Die derzeit ausgelieferten Lizenzcodes gelten für die jeweiligen Produkte für das gesamte Lizenzjahr (bis 30.11.2005).

Studierenden unter unseren **infoforum**-Lesern, die an einer Einführung in die Nutzung eines Statistik-Pakets interessiert sind und in naher Zukunft eine entsprechende Auswertung durchführen müssen, möchte ich mit Nachdruck unser Jubiläumsangebot der SPSS-Lehrveranstaltung im Sommersemester 2005 (www.uni-muenster.de/ZIV/Lehre/2005_Sommersemester/k16.html) empfehlen. In der Betreuung der Anwendungspakete haben wir schon frühzeitig in Lehrveranstaltungen auf vorliegende Programmpakete und Prozeduren hingewiesen und damit auch das SPSS in der WWU bekannt gemacht – zu Zeiten, als noch nicht einmal Handbücher erhältlich waren. Bezüglich SPSS wurde damals u. a. die Prozedur zur Faktorenanalyse nachgefragt. In dieser Entwicklung wurde dann im Sommersemester 1975 erstmals eine Lehrveranstaltung ausschließlich zum SPSS abgehalten. Wir können also auf 30 Jahre SPSS-Lehrveranstaltungen zurückblicken.

Als dienstältester lokaler SPSS-Koordinator erlaube ich mir den Nachsatz: Fassen Sie unsere Ankündigungen zum SPSS nicht als einfältige Werbung für die Produktpalette SPSS auf – wer uns kennt, der weiß sehr wohl, dass wir selbst die uns vorgelegten Probleme in der Regel im Programmsystem eines Mitbewerbers formulieren.

Suchmaschinen an der Universität Münster

R. Perske

Dieser Artikel berichtet kurz über Geschichte und aktuellen Stand der zentralen WWW-Suchmaschine.

Vor etlichen Jahren wurde an der Universität Münster eine einfache Volltextsuche „Queryindex“ entwickelt. Auf den teilnehmenden WWW-Servern lief regelmäßig ein Programm, welches eine Liste aller Wörter und statischen HTML-Dateien aufstellte und diese Liste per FTP oder NFS auf den zentralen Server übertrug. Der WWW-Leser konnte in ein einfaches Formular Wörter oder Wortanfänge eintragen, woraufhin ein kleines Programm eine WWW-Seite mit den Titeln und Adressen aller erfassten Dateien ausgab, in denen alle vom Nutzer angegebenen Wörter oder Wortanfänge vorkamen, sortiert nach Worthäufigkeiten.

Dieser Mechanismus war sehr erfolgreich und wird in Sonderfällen auch jetzt noch eingesetzt, genügte aber zuletzt nicht mehr den gestiegenen Anforderungen, da weder die rapide steigende Zahl dezentraler WWW-Server noch die wachsende Menge dynamisch erzeugter Seiten erfasst werden konnten.

Angesichts der Angebote großer Suchmaschinen-Anbieter stellte sich die Frage, ob eine eigene Suchmaschine überhaupt noch Sinn hat. Da aber eine lokale Suchmaschine geänderte Informationen sehr viel schneller und kompletter erfassen kann, entschied das ZIV sich, dazu eine neue, bessere lokale Suchmaschine mit freier Software aufzubauen, sowohl als Angebot an alle Besucher der WWW-Seiten von Universität und Universitätsklinikum als auch, um dem Wunsch vieler Informationsanbieter nach einer auf das jeweilige Angebot zugeschnittenen Suchmöglichkeit nachzukommen.¹

Im vorigen Jahr wurde deshalb die vielbenutzte Software „ht://dig“ installiert, leider stellte sich erst in der letzten Erprobungsphase heraus, dass diese Software einen erst

¹ Informationen für interessierte Informationsanbieter: <http://www.uni-muenster.de/ZIV/Hinweise/InformationenAnbieten.html#suchen>

beim Umfang der Informationen von Universität und Universitätsklinikum auftretenden Fehler aufweist.

Anschließend fiel nach gründlicher Recherche die Wahl auf „ASPseek“, eine frei verfügbare Software russischer Entwickler. Diese Software wurde auch erfolgreich installiert und in Betrieb genommen. Leider stellten sich erst nach längerem Produktionsbetrieb technische Probleme heraus, welche uns vor etlichen Wochen dazu zwangen, die Entscheidung zum erneuten Wechsel der Software zu treffen.

Nach diesem doppelten Missgeschick fiel die Wahl auf „mnoGoSearch“, ebenfalls eine russische Entwicklung. Diese Software war zum Zeitpunkt der Wahl von „ASPseek“ unterlegen, wurde aber in der Zwischenzeit kräftig weiterentwickelt und hat „ASPseek“ deutlich überholt. Die Beseitigung anfänglicher Probleme hat dank schneller Antworten der Entwickler gut geklappt. Die Inbetriebnahme von „mnoGoSearch“ ist jetzt im Wesentlichen abgeschlossen; es stehen allerdings noch Optimierungsarbeiten an.

Im Wesentlichen bietet „mnoGoSearch“ die gleichen Möglichkeiten, wie man sie auch von den großen Internet-Suchmaschinen kennt, sogar eine brauchbare Relevanzsortierung und die Erfassung von PDF-, Word-, Excel- und PostScript-Dateien. Anstelle einer Aufzählung der Suchmöglichkeiten darf ich Sie einfach bitten, die neue Suchmaschine unter <http://suche.uni-muenster.de> selbst auszuprobieren. Beachten Sie dort den Link auf die erweiterte Suche.

Bereits von vielen Informationsanbietern genutzt wird die Möglichkeit, die Suchmaschine auch für eine beschränkte Suche nur in den Informationen dieses Anbieters zu benutzen und dabei auch das WWW-Seitenlayout des jeweiligen Anbieters zu verwenden; diese Möglichkeit ist keineswegs auf die Angebote auf den zentralen WWW-Servern beschränkt.²

Natürlich bleibt die Entwicklung hier nicht stehen: Die Zukunft wird hochwertige Informationsmanagement- und -retrievalsysteme bringen, welche sehr viel effektiver als herkömmliche Suchmaschinen beim Auffinden von Informationen helfen.

Aber sicherlich werden lokale Suchmaschinen auch neben globalen Suchmaschinen wie „Google“ und neben solchen hochwertigen Retrievalsystemen ihre Existenzberechtigung behalten: Lokale Suchmaschinen erfassen die lokalen WWW-Angebote viel schneller und kompletter als globale Suchmaschinen und es entstehen anders als bei hochwertigen Retrievalsystemen keine nutzungsabhängigen Kosten.

Uni Münster setzt auf SIP

L. Elkemann

Das Uni-Telefonnetz entwickelt sich in Richtung Voice over IP (VoIP: „Stimme über Internet-Protokoll“).

Bereits bei der Inbetriebnahme 1996 zählte das Telekommunikations-Netzwerk (Tk-Netzwerk) des Hochschulstandorts Münster zu einer der imposantesten Installationen, die an deutschen Hochschulen realisiert wurden. Seither ist es beständig gewachsen – und auch die technische Weiterentwicklung der Systeme wurde vorangetragen. Mit dem neuen Software-Release werden die jetzigen Telekommunikationssysteme VoIP-fähig sein. Was das genau bedeutet, und welcher Teil des „Tk-Netzwerks“, eingebunden in das LAN, VoIP-fähig ist, soll im weiteren Verlauf etwas verdeutlicht werden.

Standards und Protokolle verfügbar?

Das Tk-Netzwerk, welches diverse Einrichtungen wie das UKM, die FH, die Kunstakademie und *last but not least* die gesamte Universität mit Sprachdiensten versorgt, ist u. a. so konzipiert, dass bei Teilnehmerumzug innerhalb des Verbundes die jetzige, bestehende Telefonnummer beibehalten werden kann.

Gewährleistet wird dies durch die Tatsache, dass zwischen den einzelnen Tk-Systemen Verbindungen bestehen, auf denen nicht nur die Sprachkanäle bereitgestellt werden,

² Dank einer von der Universitäts- und Landesbibliothek gefertigten Vorlagendatei können die Suchergebnisse auch im XML-Format ausgegeben und somit maschinell weiterverarbeitet werden.

sondern auch diverse wichtige Status- und Synchronisationsinformationen der einzelnen Tk-Systeme und Endgeräte übertragen werden. Wichtige Informationen wie Zustand der einzelnen Tk-Anlage, Gebührendaten, Zustand der Endgeräte werden ebenfalls übertragen. Grundlage hierfür ist ein proprietäres, herstellerspezifisches Protokoll, durch welches zur Zeit ca. 400 Leistungsmerkmale realisiert werden. Ein großer Teil dieser Leistungsmerkmale wird sowohl vom einzelnen Teilnehmer als auch von den Administratoren benötigt.

Unter anderem ist dadurch gewährleistet, dass das gesamte Netz von einer zentralen Stelle administrierbar und konfigurierbar ist – unter Kostengesichtspunkten, welche heute und zukünftig immer stärker zu beachten sind, ein ganz wichtiger Faktor. Ein umfangreiches Kabelnetz, bestehend aus einer Fülle von Kupfer- und Lichtwellenleiterkabeln bildet das Rückgrat dieses Tk-Netzwerks.

Parallel zu diesem Tk-Netzwerk existiert ein so genanntes *Local Area Network*, kurz LAN. Rückgrat des LAN ist ein hoch performantes und verfügbares Lichtwellenleiterkabelnetz. Auch das LAN ist zentral administrierbar und konfigurierbar. Somit betreibt der Hochschulstandort Münster zur Zeit zwei sehr gut ausgebaute Netze, die jeweils instand gesetzt und gewartet werden müssen. Dieses resultiert aus der Tatsache, dass es einige wesentliche Unterschiede in den Anforderungen an die Netze gibt. Das Tk-Netzwerk ist ein leitungsvermittelter Netze im Gegensatz zum LAN, welches ein paketvermittelter Netze darstellt. Nach erfolgreichem Verbindungsaufbau wird in einem leitungsvermitteltem Netze der Applikation, hier der Sprache, eine Ende-zu-Ende-Kommunikation über einen Kanal garantiert. Dieser Kanal ist ausschließlich für diese Verbindung geschaltet worden. Nach Abbruch dieser Verbindung wird der Kanal wieder abgebaut.

Die Daten werden transparent übertragen und treten nicht in Konkurrenz mit Daten anderer Applikationen. Dieses ist bei Echtzeitapplikationen, wie der Übertragung von Sprach- und Videodaten von entscheidender Wichtigkeit.

Anders sieht es in einem paketvermitteltem Netze aus. Die echtzeitrelevanten Daten können durchaus, je nach Topologie des Netzes, unterschiedliche Wege zum Ziel gehen. Standards und Mechanismen wie IEEE 802.1 p/Q (Layer 2) und DiffServ (Layer 3) können eine Priorisierung der Daten, was die Bevorzugung der Reihenfolge der Datenübertragung betrifft, veranlassen. Somit kann gewährleistet werden, dass zeitkritische Daten nicht in Konkurrenz treten müssen mit zeitlich unkritischen Daten. Diese Mechanismen müssen sowohl von den Applikationen als auch von der Netzhard- und -software unterstützt werden.

Die VoIP-Welt wird zur Zeit von zwei Protokollen beherrscht. Zum einen ist das Protokoll H.323 der ITU (International Telecommunications Union) zu nennen, zum anderen das Protokoll SIP (Session Initiation Protocol) der IETF (Internet Engineering Task Force), RFC 3261. Diese sind die zur Zeit wichtigsten Standards, durch welche u. a. die Funktionen einer Tk-Anlage auf dem LAN realisiert werden können. Bereits heute sind eine Fülle von Leistungsmerkmalen in den Standards realisiert. Mittels so genannter Gateways (H.323 oder SIP oder Geräte, die beide Protokolle unterstützen) wird physisch die Kopplung der beiden Netze erfolgen. Mit dem neuen Software-Release [Call@Net](#), welches auf den jetzigen Tk-Systemen installiert ist, werden SIP-fähige Gateways unterstützt, unter Beibehaltung des offenen Rufnummernplans.

VPN-Verbindungen mit Firewall unter Linux

A. Scheffer

Auf vielfachen Wunsch von Linux-Nutzern sei hier eine Dokumentation zum Aufbau einer VPN-Verbindung unter Linux vorgestellt. Die Ausführungen über Router gelten ausdrücklich nur für ein heimisches Netz und dürfen für das Uni-Netz nicht angewendet werden.

Dieser Artikel beschreibt ausführlich, wie mit einer Linux-Distribution eine VPN-Verbindung zur WWU aufgebaut werden kann. Hierfür konfigurieren wir zunächst den Paketfilter von Linux mittels `iptables` und bauen dann die Verbindung auf. Wir begnügen uns im Weiteren damit, Netzwerkverbindungen wenig detailliert als Verkehr von Datenpaketen mit Absender- und Zieladressen zu beschreiben. Eine so genannte IP-Adresse besteht dabei aus vier durch drei Punkte getrennten ganzen Zahlen zwischen 0 und 255. Für das Folgende empfiehlt es sich, alle Befehle bzw. das Skript zunächst in einer Root-Shell auszuführen (Fachkundige sollten alles in ein Runlevel-Skript auslagern).

Absicherung gegen nicht angeforderte Datenpakete

Wir stellen also zunächst sicher, dass über die spätere Verbindung keine ungebetenen Pakete den Weg auf unseren Rechner finden. Dafür konfigurieren wir den in Linux integrierten Paketfilter, welcher uns wenigstens ein Minimum an Sicherheit vor externen Angriffen bieten wird. (Besser noch ist es, man aktiviert die Firewall der verwendeten Linux-Distribution. Fachkundige können das Folgende als groben Hinweis für die dort notwendigen Einstellungen betrachten.) Wir wollen zunächst dafür sorgen, dass eingehende und weiterzuleitende (Daten-)Pakete (z. B. aus dem Internet) abgewiesen werden, während (von unserem Rechner) ausgehende Pakete zu akzeptieren sind. Hierfür setzen wir so genannte CHAIN-Policies, welche das Grundverhalten des im Kernel von Linux integrierten Filters festlegen. Hierfür findet wie angedeutet der Befehl `iptables` Verwendung:

```
iptables -P INPUT DROP && iptables -P FORWARD DROP && iptables
-P OUTPUT ACCEPT
```

Dies schützt jedoch leider vor allen eingehenden Paketen (DROP-Policies) und ist damit zu streng für den eigenen Zugriff z. B. per Browser auf das Internet. Das liegt daran, dass – nachdem eine Seiten-Anfrage abgeschickt wurde – die passende Antwort abgewiesen wird. Wir müssen bei aus dem Internet eingehenden Paketen also zwischen solchen unterscheiden, deren Eintreffen wir selbst „angezettelt“ haben, und „ungebetenen“ Paketen. Pakete zum Verbindungsaufbau (*state* NEW) akzeptieren wir nicht aus dem Internet, sonst aber schon:

```
iptables -A CHAIN -m state --state ESTABLISHED,RELATED -j AC-
CEPT
iptables -A CHAIN -m state --state NEW -i $INTERNET-INTERFACE
-j DROP
iptables -A CHAIN -m state --state NEW -j ACCEPT
```

Dies ist sowohl für die FORWARD-CHAIN, in welcher die weiterzuleitenden Pakete auflaufen, als auch für die INPUT-CHAIN durchzuführen. Als eingehende Schnittstellen kommen sowohl der Netzwerkanschluss zum Internet als auch alle PPP-Verbindungen ins Internet in Frage – die zweite Zeile taucht im endgültigen Skript also zweimal auf (s. u.). Der folgende letzte `iptables`-Befehl dient zunächst nur dazu, die Zerstückelung großer Pakete zum Transport (*fragments*) für unseren Filter transparent zu machen – wir erklären ihn im Folgenden noch genauer.

```
iptables -A POSTROUTING -t nat -o $INTERNET-INTERFACE -j
MASQUERADE
```

Nachdem wir nun für einen minimalen Schutz vor Angriffen gesorgt haben, machen wir uns an die Einrichtung einer Internet-Verbindung über VPN. Wir setzen im Weiteren voraus, dass in unserem Fall die mit dem Internet verbundene Netzwerkkarte die Kennung `eth0` vom verwendeten Linux erhält. Genauere Auskunft gibt hier der Befehl `ifconfig`, welcher die aktivierten Karten und bei aktiviertem DHCP (hierbei bekommt ein Heimrechner seine Adresse von einem Server automatisch zugeteilt – dies ist z. B. bei den VPN-Zugängen der WWU der Fall) auch gleich die zugewiesene IP-Adresse anzeigt. Wer Schwierigkeiten mit der Einrichtung seiner Wireless-LAN-Karte

hat, probiere zudem einmal den Befehl `iwconfig mode Managed essid Funk-Hoer1`.

Aufbau der VPN-Verbindung

Nun soll der Rechner eine VPN-Verbindung über die Internet-Netzwerkkarte aufbauen. Hierzu wird ein weiteres Protokoll auf die normale Verbindung aufgesetzt: PPTP. Da das Protokoll eine Punkt-zu-Punkt-Verbindung zwischen VPN-Server und Heimrechner voraussetzt, stützt sich dieses wiederum auf das P(oint to)P(oint)P(rotocol) ab. Das T im Kürzel deutet darauf hin, dass ein so genannter Tunnel aufgebaut wird. Die PPTP-Verbindung stellt mit diesen Tunnel „durch“ die normale Netzwerkverbindung über `eth0` ein virtuelles PPP-Interface (`ppp0`) bereit, welches (per DHCP) eine IP-Adresse aus dem Segment des Providers erhält. Der Rechner befindet sich so praktisch im lokalen Netz dieses Providers. Ihm wird damit erhöhtes Vertrauen entgegengebracht, und er darf folglich z. B. Drucker verbinden und Webseiten lokaler Bibliotheken anfordern. Für die Einrichtung einer PPTP-Verbindung muss das PPTP-Paket installiert sein (dies ist eigentlich bei allen aktuellen Distributionen der Fall). Wir müssen als Vorbereitung in der Datei `/etc/ppp/chap-secrets` unser Netzzugangspasswort hinterlegen, welches zuvor einmalig auf der Webseite <https://www.nic.uni-muenster.de/-Netzzugangspasswort> einzutragen ist. Die Datei `chap-secrets`, welche nur für `root` lesbar sein sollte, erhält nun (mit einem beliebigen Texteditor, z. B. `joe`) eine Zeile der Form:

```
NUTZERKENNUNG * "NETZZUGANGSPASSWORT" *
```

Der Aufbau einer VPN-Verbindung gelingt dann mit den folgenden Befehlen. Zunächst ist für den Tunnel die Route zum VPN-Router über `eth0` zu sichern:

```
route add -host VPN-ROUTER gw VPN-GATEWAY dev eth0
```

Dann bauen wir die PPTP-Verbindung auf:

```
pptp VPN-ROUTER -pap defaultroute replacedefaultroute
name beratung
```

Die `pppd`-Parameter `replacedefaultroute` und `defaultroute` sorgen dafür, dass alle Pakete jetzt über die PPTP-Verbindung, anstatt direkt über die Netzwerkkarte laufen. Der Parameter `name` setzt den Namen des Rechners und muss derselbe sein, wie in den `chap-secrets` angegeben (unsere Nutzerkennung). Da keine gesonderte Nutzerkennung angegeben wird, wird als Kennung dann auch der Rechnername verwendet. Der Parameter `-pap` ist nur für Debian-Linux notwendig und z. B. bei SUSE-Linux wegzulassen.

Das fertige Skript mit einer kleinen Liste der wichtigsten VPN-Router und Gateways wird im folgenden Kasten gezeigt (da die gleichen Befehle für FORWARD- und INPUT-Chain ausgeführt werden, sind sie dort in die Unterprozedur `ruleset` ausgelagert).

Abschließend noch ein ganz wichtiger Punkt: Ein Sicherheitskonzept geht nur dann auf, wenn es alle 24 Stunden des Tages abdeckt. Eine Firewall temporär für persönliche E-Mails zu deaktivieren, ist, wie wenn Deutschland zwei Tage im Jahr den Bundesgrenzschutz beurlaubt. Wer Dienste dem Internet zugänglich machen will, muss kleine Löcher in seine Firewall schlagen. Nahezu jede Firewall bietet dafür einen komfortablen Dialog mit einer Liste der möglichen Dienste an. Wer einen Router verwendet, muss im Konfigurationsdialog noch einen Zielrechner angeben und nutzt damit ohne sein Zutun so genanntes Port-Forwarding.

Ausblick: Routing mit Linux

Zuletzt sei noch gesagt, dass das Skript problemlos zu einer Router-Konfiguration ausgebaut werden kann. Die in die POSTROUTING-Chain eingefügte Regel hat eigentlich einen anderen Zweck, als als Nebeneffekt die Fragmentierung transparent zu machen. Weitergeleitete Pakete werden hier bis zur Rückkehr mit der per DHCP zugewiesenen IP-Adresse als Absender-Adresse versehen. Dazu kommt ein Spezialfall des Source-

NAT (Network-Address-Translation) – das sogenannte Masquerading – zum Zuge. Zum Einsatz als Router ist, da die FORWARD-Chain auch ruleset durchläuft, nur noch das IP-Forwarding zu aktivieren (`echo 1 > /proc/sys/net/ipv4/ip_forward`), welches den Wechsel von Paketen auf andere Netzwerkinterfaces erlaubt. Auch Port-Forwarding ist ohne Weiteres zu etablieren. Analog zum Masquerading ist hier die PREROUTING-Chain und Destination-NAT zu verwenden. (Interessierte mögen mit einer Suchmaschine nach den Begriffen DNAT, iptables und Linux suchen).

```

Arne@ZIVPC320:~ - Befehlsfenster - Konsole
Sitzung Bearbeiten Ansicht Lesezeichen Einstellungen Hilfe
IW fwupn Row 1 Col 1 5:41 Ctrl-K H for help
##### Filter konfigurieren #####
iptables -F # Reset
iptables -t nat -F
iptables -P OUTPUT ACCEPT # Policies setzen
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -N ruleset # Regeln als Unterprozedur anlegen
# Pakete selbst initiiertes Verbindungen akzeptieren
iptables -A ruleset -m state --state ESTABLISHED,RELATED -j ACCEPT
# Verbindungen aufbauende Pakete aus dem Netz nicht akzeptieren
iptables -A ruleset -m state --state NEW -i eth0 -j DROP
iptables -A ruleset -m state --state NEW -i ppp0 -j DROP
iptables -A ruleset -m state --state NEW -j ACCEPT
# Regelsatz ruleset einbinden
iptables -A INPUT -j ruleset && iptables -A FORWARD -j ruleset
# Fragmentierung transparent machen
iptables -A POSTROUTING -t nat -o ppp0 -j MASQUERADE

##### UPN-Verbindung aufbauen #####

# mögliche Werte für UPN-ROUTER & UPN-GATEWAY
# FunkLAN 172.16.32.1 172.16.128.2
# pLANet 172.16.72.1 172.16.160.2
# Teleport-DSL 172.16.0.1 172.16.192.2
# -----
# Host-Route sichern
route add -host UPN-ROUTER gw UPN-GATEWAY dev eth0
# PPTP-Verbindung aufbauen
pptp UPN-ROUTER -pap defaultroute replacedefaultroute name NUTZERKENNUNG
    
```

Abb. 6

Nutzung öffentlicher und privater Subnetze im LAN der Universität

M. Kamp

Die zunehmende Nutzung so genannter „privater IP-Adressen“ im Netz der Uni Münster führt zu manchen Unklarheiten, die in diesem ersten Artikel ausgeräumt werden sollen.

Im Netz der Uni-Münster werden IP-Adressen aus verschiedenen Bereichen verwendet. Dazu zählt der „öffentliche Bereich“ mit Adressen zwischen 128.176.0.0 und 128.176.255.255, der der Universität 1988 durch IANA (Internet Assigned Numbers Authority) zur Verfügung gestellt wurde. Adressen aus diesem Bereich sind, soweit keine zusätzlichen einschränkenden Maßnahmen ergriffen werden, aus dem gesamten Internet erreichbar.

Daneben gibt es auch Adressbereiche, die nicht im Internet weitergeleitet werden, sondern für die Nutzung ausschließlich in lokalen Netzen reserviert sind. Es handelt sich um die Bereiche 10.0.0.0 bis 10.255.255.255, 172.16.0.0 bis 172.31.255.255 und 192.168.0.0 bis 192.168.255.255. Diese und einige weitere reservierte Adressblöcke werden im RFC 3330 „Special-Use IPv4 Addresses“ beschrieben (www.ietf.org/rfc/rfc3330.txt). Innerhalb des Netzes der Uni Münster können diese Adressen in bestimmtem Rahmen kommunizieren, müssen aber beim ZIV besonders beantragt werden.

Um die oft unnötige Verwendung öffentlicher IP-Adressen zu vermeiden, aber auch um Endsysteme vor dem direkten Zugriff aus dem Internet zu schützen, werden diese privaten Adressen inzwischen in immer größerem Umfang auch im LAN der Universität genutzt. Allerdings muss die Nutzung hier unbedingt vom ZIV koordiniert werden, damit es zu keinen Überschneidungen von Adressen im Netz kommt und die Adressräume für kommende netzseitige Schutzmaßnahmen bereichsweise zusammengefasst werden können.

Auch Server des ZIV, die nur im Netz der Uni zugänglich sein müssen, wurden inzwischen auf private Adressen umgestellt. Hier ergibt sich das Problem, dass notwendige Windows-Updates oder aktuelle Virus-Dat-Files, die vorher über das Internet zu erhalten waren, nicht mehr erreicht werden können. Daher müssen diese Server jetzt wiederum lokale Server nutzen, um an diese Daten heranzukommen, z. B. den Microsoft Software Update Service (siehe den Artikel „SUS am ZIV“ in [infoforum](#) Nr.2/2004). Dieses gilt natürlich nicht nur für Server, sondern auch für Arbeitsplatzrechner, die auf private Adressen umgestellt werden.

Ein wachsendes Problem ist hierbei der Betrieb von „universitätsöffentlichen“ Web-Servern, also Web-Servern, die nur aus dem Netz der Universität genutzt werden dürfen. Hier wird der Zugriff meist auf Adressen aus dem öffentlichen Bereich (128.176.0.0 bis 128.176.255.255) durch Filter auf diesen Servern eingeschränkt. Arbeitsplätze in geschützten privaten Subnetzen, etwa in der Universitätsverwaltung oder im Klinikum (UKM) können auf so konfigurierte Server nicht mehr zugreifen. Hier sollten von den Web-Server-Administratoren auf jeden Fall auch die privaten Adressbereiche als universitätszugehörig betrachtet und somit zugelassen werden.

Private Adressen können nur in Absprache mit dem ZIV genutzt werden – selbst wenn es sich „nur“ um eine interne Punkt-zu-Punkt-Verbindung bei einem Cluster-Server handelt. Auch diese Verbindung hat einen Einfluss auf das interne Routing des Servers, Verbindungen in die Universität etc. zu privaten Adressen können dann möglicherweise nicht mehr aufgebaut werden. Solche Punkt-zu-Punkt-Verbindungen ohne Anbindung an das öffentliche Netz sollten besser mit einer so genannten „LinkLocal-Adresse“ aus dem Bereich 169.254.0.0 bis 169.254.255.255 versehen werden (siehe RFC 3330), LinkLocal-Adressen brauchen nicht im ZIV angemeldet zu werden, soweit die Infrastruktur des LANs nicht genutzt wird. Adressen aus diesem Bereich werden auch von verschiedenen Betriebssystemen (Win 98, ME, XP, MacOS) verwendet. Das von Microsoft verwendete Verfahren mit dem Namen „APIPA“ (Automatic Private IP-Adressing) prüft alle fünf Minuten ob per DHCP eine IP-Adresse bezogen werden kann. Solange dies nicht gelingt, verwendet das System eine zufällige Adresse aus dem Bereich 169.254.0.0/16, wobei vorher geprüft wird ob diese Adresse nicht schon von einem anderen System verwendet wird.

Ein ähnliches Verfahren gibt es auch unter MacOS unter der Bezeichnung „Rendezvous“. Diese Adressen haben aber nur einen Sinn, wenn das entsprechende Subnetz ausschließlich für Rechnerperipherie, wie z. B. Fire-Wire-Geräte (Kameras u. a.), mitnutzende PDAs über USB usw. verwendet wird.

DFNVC – der Videokonferenzdienst im deutschen Wissenschaftsnetz

G. Maiss

Diesen Artikel drucken wir mit freundlicher Genehmigung des DFN-Vereins ab.

Der DFN-Verein bietet den Wissenschaftlern in Deutschland die Möglichkeit, über den Videokonferenzdienst DFNVC und das Gigabit-Wissenschaftsnetz multimedial mit Kollegen an anderen Hochschulen und Forschungseinrichtungen zu kommunizieren. DFNVC ist speziell auf die Anforderungen wissenschaftlicher Nutzer zugeschnitten und kann direkt vom Arbeitsplatz aus über PCs und Laptops sowie Videokonferenz-Raumsysteme oder Telefone genutzt werden. Der Dienst ermöglicht Videokonferenzen mit einer Vielzahl von Teilnehmern und steht den Nutzern rund um die Uhr ohne vorherige Planung und Reservierung zur Verfügung. Mit einem Pauschalpreis pro Einrichtung können beliebig viele Videokonferenzen auch mit internationalen Partnern durchgeführt werden. Parallel zur Videokonferenz besteht die Möglichkeit, Arbeitsdokumente auszutauschen.

Folgende Anwendungsbeispiele illustrieren Einsatzmöglichkeiten:

Konferenzen von Rektoren, Präsidenten, Kanzlern und Leitern von Rechenzentren und anderen Einrichtungen



Programmausschuss-Sitzung der Deutschen Initiative für Netzwerkinformation (DINI)

- Direktoren oder Rechenzentrumsleiter können schnell und flexibel Entscheidungen treffen, wenn sie ihre Besprechungen über eine Videokonferenz durchführen. Auf Wunsch betreut ein Operator die Konferenz und sorgt für reibungslosen technischen Ablauf.

Übertragungen von Vorlesungen

- Studenten können Vorlesungen von zu Hause aus verfolgen oder an einem Seminar aktiv teilnehmen.

Austausch von Unterlagen / gemeinsames Bearbeiten

- Institute mit verschiedenen Standorten sind an Außenmessungen beteiligt, die Ergebnisse liegen nur an einem Standort vor. Während einer Videokonferenz werden diese Ergebnisse über ein Whiteboard angezeigt und bearbeitet.

Gemischte Video- und Telefonkonferenzen

- In einer Videokonferenz werden Forschungsergebnisse diskutiert. Ein Experte, der nicht über ein Videokonferenzsystem verfügt, oder ein Teilnehmer auf Reisen kann über das Telefon hinzugezogen werden.

Abwicklung von Auswahlgesprächen und Tests



Übertragung von Vorlesungen und Seminaren

- Für ein erstes Vorstellungsgespräch können Bewerber ohne Reiseaufwand über eine Videokonferenz eingeladen und begutachtet werden. Auf diesem Wege können auch Tests und Prüfungen durchgeführt werden.

Je nach Anwendungsumgebung kommen verschiedene Videokonferenzgeräte zum Einsatz. Will man Videokonferenzen von seinem gewohnten Arbeitsplatz aus durchführen, so muss der PC oder Laptop mit einem so genannten Desktop-System ausgerüstet werden (ab ca. 180,- Euro pro Arbeitsplatz inkl. Kamera und Headset als Software-Lösung, ab ca. 350,- Euro als Hardware-Lösung). Soll ein Seminar- oder Schulungsraum ausgestattet werden, so bieten sich so genannte Settop-Systeme mit einem Monitor an, mit denen z. B. Treffen von Arbeitsgruppen möglich werden (ab ca. 6.000,- Euro erhältlich). Etwas teurer und aufwändiger wird es bei der Ausstattung von großen Konferenzräumen mit Systemen, die über mehrere Monitore, Rollwagen und hohe Übertragungsbandbreiten verfügen.

Bei Auswahl und Einsatz von Videokonferenzsystemen bietet das vom DFN-Verein betriebene Kompetenzzentrum für Videokonferenzdienste (VCC) an der TU Dresden (vcc.urz.tu-dresden.de/) wertvolle Hilfe an. Das VCC untersucht laufend aktuelle Videokonferenzhardware und -software, erstellt Installationsanleitungen, steht für Tests

zur Verfügung und berät bei der Anschaffung und Einrichtung eines Videokonferenzsystems. Für Einrichtungen, die am Dienst DFNVideoConference teilnehmen wollen, werden Schulungen für die Betreuer in den Einrichtungen angeboten, die eine praktische Einführung in alle Bereiche der Videokonferenztechnik geben. Als Einarbeitung in die Thematik ist auch das vom VCC erstellte kostenlose Videokonferenz-Handbuch des DFN-Vereins geeignet (vcc.urz.tu-dresden.de/vc-handbuch/). Ein detaillierter Einblick in die technischen Hintergründe findet sich unter www.dfn.de/uploaded/DFNVC-Technik-Info.pdf.



Videokonferenz im Rechenzentrum der Universität Hannover

VC-Portal

Zentraler Einstiegspunkt des Dienstes ist ein vom DFN-Verein bereitgestelltes VC-Portal, das unter der Adresse www.vc.dfn.de erreichbar ist. Hier werden alle dienstrelevanten Informationen angeboten.

Haben wir Ihr Interesse geweckt?

1. Dann fragen Sie nach, ob Ihre Einrichtung einen Vertrag über die Nutzung des DFN-Videokonferenzdienstes mit dem DFN-Verein abgeschlossen hat und zu welchen Bedingungen Sie daran teilnehmen können. Nehmen Sie Kontakt zu dem entsprechenden Administrator in Ihrem Rechenzentrum auf.
2. Erkundigen Sie sich, ob es in Ihrer Hochschule ein Videokonferenzsystem gibt, an dem Sie zunächst unter Anleitung an einer Videokonferenz teilnehmen können, bevor Sie an die Installation eines eigenen Systems gehen.
3. Statten Sie sich mit einem Videokonferenzsystem aus. Wir beraten Sie gerne dabei. Alle notwendigen Daten zur Installation und Konfiguration erhalten Sie in Ihrer Einrichtung oder bei der DFN-Hotline.
4. Nach erfolgreicher Konfiguration und Anmeldung Ihres Videokonferenzgerätes kann es losgehen: Sie wählen eine Konferenznummer und treffen sich mit Ihren Konferenzpartnern in einer Videokonferenz.

Haben Sie Fragen?

Schauen Sie nach unter „Dienstleistungen / DFNVC“ auf den DFN-Seiten www.dfn.de oder auf dem VC-Portal unter www.vc.dfn.de oder melden Sie sich bei der Hotline unter hotline@vc.dfn.de.

Die neuen Multimedia-Räume des ZIV

A. Scheffer, H.-W. Kisker

Die Behandlung des Themas Multimedia im ZIV stößt auf breite Akzeptanz, wie vor allem die sehr gut angenommenen Vorlesungen und Praktika dazu belegen. Deshalb wurden zusätzlich zu den Scanner-Arbeitsplätzen in der Benutzerberatung vier neue Multimedia-Arbeitsplätze eingerichtet. Diese erweitern das Angebot um Digitalisierungsgeräte und Bearbeitungsmöglichkeiten für Dias, Filme u.v.m.

Nachdem das diessemestriges Multimedia-Praktikum schon anderthalb Monate in den neuen Multimedia-Räumen stattfindet, meinen wir nun genug Erfahrungen gesammelt zu haben, um die beiden Räume im ZIV-Gebäude Einsteinstraße auch in größerem Umfang der Öffentlichkeit vorzustellen. Für Interessierte sei es gleich vorweg gesagt: In der Sonderausgabe des **infoforum** wird das Thema Multimedia im ZIV umfassender dargestellt, das Nachfolgende geht im Wesentlichen auf die neuen Geräte und das Nutzungsverfahren ein.

Räumlichkeiten und Geräte

Es gibt im ZIV zwei Multimedia-Räume mit je zwei Rechnern. Insgesamt stehen also vier Arbeitsplätze zur Verfügung. In den Räumen existieren zudem PLANet-Anschlüsse (USB und Twisted Pair) für den Einsatz eigener Notebooks.

Jeder dieser Arbeitsplätze ist mit

- zwei Monitoren (einer für die Anleitungen),
- einem Smart-Karten-Lesegerät,



Abb. 7

- einem CD/DVD-Brenner,
- einem Lesegerät für die Speicherkarten digitaler Kameras und
- an der Frontseite der Rechner gut zugänglichen Schnittstellen für USB- und FireWire ausgestattet.

Des Weiteren stehen folgende Geräte zur Verfügung:

- ein Scanner Epson 3170 mit Blatteinzug für automatisches Scannen von bis zu 30 Seiten,
- ein Dia-Scanner Reflecta DigitDia 3600 zum automatischen Scannen von bis zu 200 Dias in handelsüblichen Magazinen,
- ein Film-Scanner Canon FS 4000US zum Scannen von Dias, Negativen und APS-Filmen in sehr guter Qualität,
- ein Flachbettscanner Epson Perfection 2400 Photo zum Scannen von Papierfotos und
- ein Video-Recorder Panasonic zum Digitalisieren analoger Video-Bänder und deren Umwandlung in Video-DVDs.

Ein Scanner mit Buchkante zum schonenden und unverzerrten Lesen gebundener Bücher und ein CD-Drucker zum Bedrucken von entsprechend beschichteten CD- bzw. DVD-Rohlingen werden demnächst noch hinzukommen.

Die verwendeten Geräte sind weitgehend in eine farbkalibrierte Umgebung eingebunden. Zumindest in einem Raum sind auch Lampen und Möbel auf Farbkalibrierung hin ausgesucht.

Die erarbeiteten Materialien werden auf den Arbeitsgeräten lokal zwischengespeichert. Am Ende einer Sitzung müssen sie von hier kopiert werden. Sie können auf eine CD bzw. DVD gebrannt oder aber auch auf einen privaten USB-Stick kopiert werden. Natürlich können Sie auch über das Netz in ein privates Home-Verzeichnis gespeichert werden.

Das Nutzungsverfahren – oder: Wie buche ich einen Multimedia-Arbeitsplatz?

Im Regelbetrieb (außerhalb der reservierten Praktikumszeiten) kann jeder Universitätsangehörige einen Multimedia-Arbeitsplatz für einen halben Tag über ein Web-Formular

für sich reservieren (siehe Nutzungsverfahren). Dies geschieht unter: <http://www.uni-muenster.de/ZIV/mmimziv.html>.

Nachdem man sich mit Benutzernamen und Standardpasswort angemeldet hat, erscheint eine Seite der folgenden Abbildung.

Als **Nutzer** können Sie Reservierungen vornehmen oder wieder aufheben.

In der folgenden Tabelle können Sie durch Anhaken oder Entfernen eines Hakens eine Reservierung vornehmen bzw. aufheben. Sie können auch zu anderen Wochen sequenziell oder per Kalender navigieren. Die Buchstaben A bis D beziehen sich auf folgende Rechner:

- A: Ringnebel (Video-Grabber/-Recorder)
- B: Andromeda (Papierstapel-Scanner)
- C: Plejaden (Diamagazin-Scanner, Film-/Dia-Scanner)
- D: Saturn (A4-Scanner)

2004	Mo, 06.12.				Di, 07.12.				Mi, 08.12.				Do, 09.12.				Fr, 10.12.			
Platz	A	B	C	D	A	B	C	D	A	B	C	D	A	B	C	D	A	B	C	D
9-12 Uhr	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13-16 Uhr	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Abb. 8

Auf dieser Seite kann nun einfach durch Wählen eines Halbtages (nach Datum) und Anhaken der entsprechenden Rechner-Geräte-Kombination gebucht werden („Übernehmen“ klicken nicht vergessen!). Einen Schlüssel für den Raum bekommt man zu Beginn der gebuchten Zeiten bei Herrn Scheffer im Zimmer 112 oder (ab 10 Uhr) in der Benutzerberatung direkt neben den beiden Multimedia-Räumen.

Wer hilft mir bei der Nutzung der Geräte und bei allgemeinen Fragen?

Unterstützung bei der Anwendung der Geräte findet der Nutzer zunächst auf den Webseiten des ZIV: Das „Multimedia-Portal des ZIV“ unter: <http://MMimZIV.uni-muenster.de> ist sowohl bei Arbeiten in den Multimedia-Räumen als auch für das Multimedia-Praktikum die zentrale Informationsquelle (siehe Abb. 9). Geräte und Anwendungsmöglichkeiten werden dort umfassend (und auch für Anfänger verständlich) beschrieben. Manche Themen sind darüber hinaus so dargestellt, dass sie auch von allgemeinem Interesse sein können. Sollten Fragen unbeantwortet bleiben, so hilft das Multimedia-Team natürlich auch nach der Schlüsselausgabe gerne weiter. Gerade im jetzt anlaufenden Betrieb sind zudem Erfahrungen und Anregungen immer willkommen.

Multimedia im ZIV von Hans-Werner Kisker

Multimedia im ZIV

Service **Beratung** mein ZIV Lehre Systeme Organisation

IKM-Service

MM im ZIV

- > Die MM-Räume
- > Das MM-Praktikum
- > Artikel
- > Kurzanleitungen
- > Digitale Fotografie
- > Scanner
- > Video
- > Bilder im Internet
- > Geräte
- > Software
- > Download
- > Handbücher



Willkommen im Multimedia-Portal des Zentrum für Informationsverarbeitung!

Das Portal bietet Zugang zu den folgenden Themenbereichen:

 Die MM-Räume	 Das MM-Praktikum	 Artikel	 Itinerarien (Kurzanleitungen)
 Digitale Fotografie	 Scannen	 Video	 Bilder aus dem Internet
 Gerätebeschreibungen	 Software-Anleitungen	 Downloads	 Bibliothek

ZurückblätternDiese Seite:   © 2004 Zentrum für InformationsverarbeitungSeitenanfang

Abb. 9

ZIV-Lehre

Veranstaltungen in der vorlesungsfreien Zeit (Frühjahr 2005)

<p>Beratung zum Lehrangebot durch Herrn W. Bosse jeweils Di, Do 11–12, ☎ 83-3 15 61</p>	<p>Für alle Veranstaltungen ist eine frühzeitige Online-Anmeldung erforderlich, die ausgehend von der Webadresse http://www.uni-muenster.de/ZIV/Content-Lehre.html unter „Anmelden zu den Veranstaltungen“ erfolgen kann. Für den Dialog sollte dabei vorzugsweise auf die dort angebotene verschlüsselte (abhörsichere) Datenübertragung umgeschaltet werden. Anmeldungen zu den Veranstaltungen sind möglich ab 6. Januar 2005 für die vorlesungsfreie Zeit, ab 1. März 2005 für die Vorlesungszeit.</p>	
<p>260018</p>	<p>Sicherheit und Schutz im Internet vom 28.02. bis 04.03.2005, Mo-Fr 10-17 Uhr Hörsaal: ZIV-Pool 3, Einsteinstr. 60</p>	<p>Perske, R.</p>
<p>260022</p>	<p>Publizieren mit LaTeX vom 07.03 bis 18.03.2005, Mo-Fr 9-16 Uhr Hörsaal: M4, Einsteinstr. 64</p>	<p>Kaspar, W.</p>
<p>260037</p>	<p>Präsentationen mit LaTeX vom 04.04. bis 08.04.2005, Mo-Fr 9-16 Uhr Hörsaal: M4, Einsteinstr. 64</p>	<p>Kaspar, W.</p>
<p>260041</p>	<p>Programmieren in Java für Fortgeschrittene vom 28.02. bis 11.03.2005, Mo-Fr 11-13 Uhr Hörsaal: M4, Einsteinstr. 64</p>	<p>Süselbeck, B.</p>
<p>260056</p>	<p>Betriebssystem Linux/Unix: Einführung und Grundlagen vom 08.02. bis 18.02.2005, Mo-Fr 10-16 Uhr Hörsaal: ZIV-Pool 3, Einsteinstr. 60 Beginn: Dienstag 08.02.2005</p>	<p>Grote, M.</p>
<p>260060</p>	<p>Systemadministration für Linux-Systeme vom 14.03. bis 18.03.2005, Mo-Fr 9-16 Uhr Hörsaal: ZIV-Pool 3, Einsteinstr. 60</p>	<p>Hölters, J.</p>
<p>260075</p>	<p>Administration eines Windows-Systems vom 21.02. bis 25.02.2005, Mo-Fr 9-17 Uhr Hörsaal: M4, Einsteinstr. 64</p>	<p>Kämmerer, M.</p>
<p>260080</p>	<p>Systemadministration für Windows-Server in einer Active-Directory-Umgebung vom 28.02. bis 04.03.2005, Mo-Fr 9-16 Uhr Hörsaal: Raum 206, Röntgenstr. 9-13</p>	<p>Lange, W. Winkelmann, O.</p>
<p>260094</p>	<p>Rechnernetze und Internet: Fortgeschrittene Themen vom 21.02. bis 25.02.2005, Mo-Fr 9-16 Uhr Hörsaal: Raum 206, Röntgenstr. 9-13</p>	<p>Richter, G. Forsmann, A. Kamp, M. Speer, M. Wessendorf, G.</p>

Veranstaltungen in der Vorlesungszeit (Sommersemester 2005)

260109	Programmieren in Java Mittwoch 13-15 Uhr Hörsaal: M4, Einsteinstr. 64, Beginn: 20.04.2005	Mersch, R.
260113	Dynamische Webseiten mit PHP und MySQL Donnerstag 9-11 Uhr Hörsaal: M4, Einsteinstr. 64, Beginn: 21.04.2005	Sturm, E.
260128	Statistische Datenanalyse mit dem Programmsystem SPSS Donnerstag 11-13 Uhr Hörsaal: ZIV-Pool 3, Einsteinstr. 60, Beginn: 21.04.2005	Nienhaus, R.
260132	Kolloquium des Zentrums für Informationsverarbeitung Freitag 14-16 Uhr Hörsaal: Raum 206, Röntgenstr. 9-13	Held, W.

Kommentare zu den Veranstaltungen

260018 Sicherheit und Schutz im Internet

Das Internet ist eine mächtige und leistungsfähige Kommunikations-Infrastruktur, birgt aber auch erhebliche Gefahren, welche für einen unbedarften Nutzer nur schwer zu erkennen sind. In der praktikumsähnlich aufgebauten Veranstaltung wird gezeigt, welche Gefahren bestehen und wie man sich ohne große Mühe vor den meisten dieser Gefahren schützen kann. Praktisch geübt werden das richtige Absichern des eigenen Rechners und die verantwortungsbewusste Verwendung geeigneter Software mit den Zielen:

- Schutz gegen Viren und andere Angriffe
- sicheres Surfen im WWW
- Sichere E-Mail
- sichere Interaktion im WWW (z. B. Online-Banking)
- sichere Dialog- und Datenverbindungen

Sicherheit umfasst dabei sowohl den Schutz des eigenen Rechners als auch Vertraulichkeit, Vertrauenswürdigkeit und Zuverlässigkeit der Kommunikation. Es wird deutlich, dass die unverzichtbaren Hilfsmittel Verschlüsselung, elektronische Unterschriften und Zertifikate viel einfacher zu benutzen sind, als man sich gemeinhin vorstellt. Vorausgesetzt werden sicherer Umgang mit E-Mail und WWW sowie Erfahrungen in der Installation und Konfiguration von Software auf dem eigenen Rechner.

260022 Publizieren mit LaTeX

LaTeX ist ein mächtiges und flexibles Satzsystem, das sich besonders für wissenschaftliche und technische Publikationen eignet. Autoren können aus einer Vielzahl von fertigen Layouts auswählen und diese eigenen Vorstellungen anpassen. Mit speziellen Komponenten, z. B. zur Erzeugung von PDF-Dateien, können LaTeX-Publikationen für die Veröffentlichung auf CD-ROM oder im Internet vorbereitet werden. Das komplette Satzsystem ist frei erhältlich und steht praktisch auf allen verbreiteten Betriebssystemen zur Verfügung.

In dieser Veranstaltung werden die Grundkonzepte und wichtigsten Erweiterungen von LaTeX vorgestellt, u. a.

- die Komponenten des Satzsystems,
- allgemeine Dokument- und Textstrukturen,

- Formeln, Tabellen, Grafiken und
- die Erzeugung von PDF-Dokumenten,

und wie hiermit ordentlich strukturierte und typografisch ansprechende Dokumente erstellt werden können.

Voraussetzung für diese Veranstaltung sind Grundkenntnisse im Umgang mit PCs.

DETIG: *Der LaTeX Wegweiser*, Thomson

NIEDERMAIR: *LaTeX – Das Praxisbuch*, Franzis'

KLÖCKL: *LaTeX2e: Tips und Tricks*, dpunkt

260037 Präsentationen mit LaTeX

LaTeX ist vor allem als ein TeX-Makropaket zur Herstellung hervorragend gesetzter Bücher bekannt. Dass aber schon die erste LaTeX-Version aus dem Jahre 1985 eine Dokumentklasse für die Herstellung von Overheadprojektorfolien enthielt, dürfte weniger bekannt sein. Dabei ist es für Arbeiten, die mit LaTeX gesetzt wurden, recht naheliegend, auch für die Präsentation LaTeX zu verwenden, um z. B. Text oder Formeln direkt übernehmen zu können. Inzwischen sind weitere LaTeX-Klassen entwickelt worden, mit denen anspruchsvolle Präsentationen erstellt und als pdf-Dateien mit dem Adobe Reader überall gezeigt werden können.

In dieser Veranstaltung wird die LaTeX-Klasse „beamer“ vorgestellt, die unter anderem eine schrittweise Anzeige des Seiteninhalts, wie z. B. Formelteile, und die Herstellung eines Handouts aus den Präsentationstexten unterstützt.

260041 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 I/O 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.

260056 Betriebssystem Linux/Unix: Einführung und Grundlagen

Linux ist ein leistungsstarkes Unix-System für viele Hardware-Architekturen. Als preiswerte Windows-Alternative ist es augenblicklich in aller Munde. Die Vorlesung will in die Linux-Benutzung einführen. Sie besteht aus zwei Teilen.

Zuerst erfolgt eine an üblichen Unix-Einführungen orientierte Beschreibung des Unix-Datei-Systems und der wesentlichen Unix-Befehle. Anschließend wird die grafische Oberfläche KDE behandelt, die für viele ein Linux-System erst attraktiv macht.

260060 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 die grundlegenden 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 Kerberos-Dienstes zur Authentisierung. Ferner wird auch die automatisierte Installation und Parametrierung einer größeren Anzahl von Linux-Systemen behandelt.

260075 Administration eines Windows-Systems

Für Hörer/innen mit Windows-Vorkenntnissen werden Arbeiten zum Aufbau und Betrieb eines Windows-Systems vorgestellt und gemeinsam erprobt.

Die folgenden Themen werden u. a. behandelt:

- Installation und Konfiguration
- Benutzer- und Gruppenverwaltung, lokale Administration
- Druck-, Datei-, Logon- und allgemeine Programm-Services
- Zugriffsrechte und Netz-Freigaben
- Diagnose- und Überwachungsfunktionen
- Internet, LAN, Netz-Protokolle
- Absicherung gegen Angriffe von außen

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 werden. Wir verweisen auf die weitere Veranstaltung „Systemadministration für Windows-Server in einer Active-Directory-Umgebung“

260080 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.

260094 Rechnernetze und Internet: Fortgeschrittene Themen

Folgende Themen sollen behandelt werden:

1. IP-Routing
2. IP-Multicast
3. virtuelle Netzstrukturen
4. Sicherheit in Rechnernetzen
5. Netzwerkmanagement
6. Ethernet-Troubleshooting
7. Zugangstechnologien

260109 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.

260113 Dynamische Webseiten mit PHP und MySQL

Diese Veranstaltung kann als Fortsetzung von „Erstellen von dynamischen Webseiten mit PHP“ angesehen werden. Kenntnisse von HTML und CSS sowie Grundkenntnisse von PHP werden vorausgesetzt. Großen Raum wird die Vorstellung der Datenbank MySQL einnehmen, weitere Themen sind Sitzungsverwaltung, Up- und Download sowie XML.

260128 Statistische Datenanalyse mit dem Programmsystem SPSS

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

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

260132 Kolloquium des Zentrums für Informationsverarbeitung

Im Rahmen des Kolloquiums werden Vorträge über aktuelle Themen der Informationsverarbeitung gehalten. Vortragstermine werden im WWW und durch Aushang bekanntgegeben.

ZIV-Regularia

Fingerprints

R. Perske

Unter dieser Rubrik erscheinen regelmäßig die aktuellen kryptographischen Prüfsummen der öffentlichen Schlüssel, die von der WWUCA und vom ZIV verwendet werden.

Bei E-Mails, WWW-Servern und an vielen anderen Stellen wird zunehmend mit Verschlüsselung und elektronischen Unterschriften gearbeitet. Dabei besitzt mindestens einer der Kommunikationspartner (beispielsweise der WWW-Server) einen öffentlichen Schlüssel, der vom anderen Partner (beispielsweise Ihrem WWW-Browser) zum Verschlüsseln oder zum Überprüfen einer elektronischen Unterschrift benutzt wird.

Um zu verhindern, dass Ihnen falsche öffentliche Schlüssel untergeschoben werden, sollten Sie überprüfen, ob der jeweilige Schlüssel tatsächlich zur angegebenen Person bzw. zum angegebenen Server gehört. Zu diesem Zweck sind die Schlüssel häufig mit Zertifikaten versehen, das sind elektronische Beglaubigungen, ausgestellt von sog. Zertifizierungsstellen, in denen die Eigentümerschaft bestätigt wird.

Im Bereich des deutschen Wissenschaftsnetzes erstellen die DFN-PCA als übergeordnete Zertifizierungsinstanz und die WWUCA als Zertifizierungsstelle der Universität Münster solche Zertifikate, siehe <http://www.dfn-pca.de> und <http://www.uni-muenster.de/WWUCA/>. Seit Januar 2004 zertifiziert die WWUCA auch RSAv4- und DSS/DH-Schlüssel, die mit GnuPG, PGP 8 u. Ä. erzeugt wurden.

DFN-PCA und WWUCA unterstützen zwei verschiedene Verschlüsselungs- und Zertifizierungssysteme: Die PGP-Familie (Pretty Good Privacy), zu der auch GnuPG (Gnu Privacy Guard) gehört, wird meistens bei E-Mail eingesetzt. Die X.509-Familie wird beispielsweise bei abhörsicheren WWW-Servern, bei S/MIME und bei Object Signing verwendet.

Zum Überprüfen der von DFN-PCA und WWUCA ausgestellten Zertifikate benötigen Sie deren öffentliche Schlüssel. Diese finden Sie auf <http://www.uni-muenster.de/WWUCA/zertifikate.html> (X.509 und PGP) oder auch an anderen Stellen wie beispielsweise der perMail-Titelseite <http://permail.uni-muenster.de> (nur X.509), der ZIVprint-Einstiegsseite <http://www.unimuenster.de/ZIV/zivprint.html> (nur X.509) oder der ZIV-Mitarbeiterliste <http://www.uni-muenster.de/ZIV/Mitarbeiter/> (nur PGP).

Die Fingerabdrücke (Fingerprints) dieser Schlüssel sind nachfolgend abgedruckt, damit Sie beim Aktivieren der Schlüssel auf Ihrem Rechner kontrollieren können, dass Sie tatsächlich die echten Zertifizierungsschlüssel erhalten haben.

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:

KeyID 4CB7658D: Zertifizierungsstelle Universitaet Muenster (E-Mail) <ca@uni-muenster.de>
 2048 Bits, Fingerprint: 383D 0F16 CEFC 1F9E B7C3 04B1 2020 FCE6
 KeyID 94E799B5: DFN-PCA (2004), ENCRYPTION Key <dfnpca@dfn-pca.de>
 2048 Bits, Fingerprint: A9F8 2DC4 09CC DA7F DC67 8FE5 28DE AAAC

PGP-Zertifizierungsschlüssel der WWUCA

KeyID 38B7A481: Zertifizierungsstelle Universitaet Muenster 2004-2005
 2048 Bits, Fingerprint: 973E 0725 040B 1745 F272 180D 08C2 C15A
 KeyID BC811EB1: Zertifizierungsstelle Universitaet Muenster 2002-2003
 2048 Bits, Fingerprint: 2864 01BC F0EF D5BA D9A0 866C 4379 4C1D
 KeyID 313C02F5: Zertifizierungsstelle Universitaet Muenster 2000-2001
 2048 Bits, Fingerprint: 3762 F5E0 C278 7697 530F 2DF2 F3B3 27F5
 KeyID EF750F1D: Rainer Perske +49(251)83-31582 Certification Key
 2048 Bits, Fingerprint: 2F38 6EF8 DC2E D85E 5B35 DB49 8AE4 52AF

PGP-Zertifizierungsschlüssel der DFN-PCA

KeyID FDCB1C33: DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2004-2005)
 <http://www.dfn-pca.de/>
 2048 Bits, Fingerprint: 96B0 AD7F B8DC 0018 DCA0 7053 1C3B 4DA5
 KeyID F2D58DB1: DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2002-2003)
 <http://www.dfn-pca.de/>
 2048 Bits, Fingerprint: DE31 690D BC6A E779 4DCD A1B5 8180 FE7B
 KeyID 63EB5391: DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2001)
 <not-for-mail>
 2048 Bits, Fingerprint: CFAF 6C29 4E57 4E0E E81C BDB4 54FD 2AAB
 KeyID F7E87B9D: DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 1999-2000)
 <not-for-mail>
 2048 Bits, Fingerprint: 6570 7274 B5E0 3FF0 EA7C ABE4 465F B8B2
 KeyID 35DBF565: DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 1997-1998)
 <not-for-mail>
 2048 Bits, Fingerprint: 097C 0919 D3C3 86DC 7A30 1511 1295 8DE3

X.509-Zertifikate der WWUCA

Inhaber: C=DE, O=Universitaet Muenster,
 CN=Zertifizierungsstelle 2004-2005/Email=ca@uni-muenster.de
 Aussteller: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA,
 CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
 Seriennummer: 64774066 (0x3dc5fb2)
 MD5-Fingerprint: 2619 6BEF 66B2 7044 52CC BE11 4C5F 3CB8
 SHA1-Fingerprint: 1765 AE6D 57C7 7914 D2AF BAF3 439C E139 66E1 A0AE

Inhaber: C=DE, O=Universitaet Muenster,
 CN=Zertifizierungsstelle 2002-2003/Email=ca@uni-muenster.de
 Aussteller: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA,
 CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
 Seriennummer: 1774668 (0x1b144c)
 MD5-Fingerprint: A431 AD41 D8F2 1856 4E31 CC69 71E6 174F
 SHA1-Fingerprint: 6945 20CA 1AFE 5CFA 6C37 52EB B772 B054 90EC D979

X.509-Wurzelzertifikat der DFN-PCA

Inhaber: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA,
 CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
 Aussteller: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA,
 CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
 Seriennummer: 1429501 (0x15cffd)
 MD5-Fingerprint: 3E1F 9EE6 4C6E F022 0825 DA91 2308 0503
 SHA1-Fingerprint: 8E24 22C6 7E6C 86C8 90DD F69D F5A1 DD11 C4C5 EA81

Alle Angaben zur DFN-PCA ohne Gewähr.

Liebe Leserin, lieber Leser,

wenn Sie **infoforum** regelmäßig beziehen wollen, bedienen Sie sich bitte des unten angefügten Abschnitts. Hat sich Ihre Adresse geändert oder sind Sie am weiteren Bezug von **infoforum** 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 **infoforum**



- 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 **infoforum**
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 **infoforum**-Leserdatei gespeichert werden (§ 4 DSGVO).

Ort, Datum

Unterschrift