Universität Karlsruhe (TH)
Rechenzentrum

juli / august 2005

RZ news

Mobile Computing

Wireless Roaming im DFN

Identity Management

KIM - Karlsruher Integriertes InformationsManagement

Security

RZ-Test: Dateisystemverschlüsselung mit Bestcrypt

Institut für Angewandte Informatik
und formale Beschreibungsverfahren

Online-Klausur mit ILIAS

Ausbildungspool im Rechenzentrum der Universität Karlsruhe (TH)

Foto: sl

ISSN 1432-7015

INHALT

IMPRESSUM

Herausgeber: Prof. Dr. Wilfried Juling
Redaktion: Ursula Scheller
Tel.: 0721/608-4865
E-Mail: scheller@rz.uni-karlsruhe.de
http://www.rz.uni-karlsruhe.de/publikationen/rz-news.php

Universität Karlsruhe (TH)
Rechenzentrum
D-76128 Karlsruhe
Nummer 7, 8 / 2005
ISSN 1432-7015

Mobile Computing

Wireless Roaming im Deutschen Forschungsnetz

Willi Fries

Universität Karlsruhe (TH) seit Juni DFN-Roaming-Partner

Angehörige der Universität Karlsruhe können seit dem 1. Juni 2005 mit dem Dial-In Account des Rechenzentrums bei allen DFN-Roaming-Partnern einen drahtlosen Zugang zu ihrem Heimatnetz herstellen. Umgekehrt haben Gäste anderer DFN-Mitgliedseinrichtungen an der Universität Karlsruhe seitdem die Möglichkeit, mit den Accounts ihrer Heimateinrichtung über DUKATH eine Verbindung zum eigenen Netz aufzubauen.

Bereits im Jahre 2002 wurde im Landeshochschulnetz BelWü ein rudimentäres Roaming zwischen den Hochschulen des Landes realisiert. Dieses Roaming erfolgt durch VPN (Virtual Private Network)-Multitunnels, d. h. jede Hochschule hat die Möglichkeit geschaffen, aus dem eigenen drahtlosen Netz einen VPN-Tunnel zu allen anderen Hochschulen aufzubauen. Dies war jedoch nur möglich, weil alle Hochschulen die gleiche VPN-Technologie (CISCO IP-Sec) einsetzten.

Die Vorteile dieser Lösung waren zum einen die einfache Realisierung und zum anderen die transparente Sicherheits-Policy. Jeder Roaming-Teilnehmer erreicht durch einen Tunnel sein Heimatnetz und ist somit seiner gewohnten Policy unterworfen. Schwierigkeiten bereitet jedoch der Wartungsaufwand bei dieser Lösung. Bei jeder Modifizierung (zum Beispiel Änderung der IP-Adresse eines VPN-Konzentrators) oder Neuanmeldung eines Roaming-Teilnehmers müssen alle Administratoren aller Einrichtungen tätig werden, um diese Änderung in den Zugangslisten nachzuziehen. Die Folge ist, dass die Aktualität der Filterlisten in den jeweiligen Einrichtungen sehr unterschiedlich ist, was wiederum dazu führt, dass die Roaming-Verfügbarkeit nicht zu hundert Prozent gegeben ist. Daher soll dieses Verfahren mittelfristig durch das DFN-Roaming abgelöst werden.

Das DFN-Roaming beruht auf einem hierarchischen Verbund von Radiusservern, dessen Wurzel vom DFN betrieben und gewartet wird. Die Authentifizierung wird bei den jeweiligen Einrichtungen durch einen Radiusserver bestätigt. Bei einem Fremdbenutzer fragt der Radiusserver den Rootserver des DFN, der wiederum die Anfrage an den zuständigen Radiusserver im Heimatnetz des Fremdbenutzers weiterleitet. Nach einer erfolgreichen Authentifizierung muss nun die Einrichtung entscheiden, welche Rechte dem Fremdbenutzer eingeräumt werden. Darin liegt auch die Problematik dieses Verfahrens. Der Fremdbenutzer befindet sich netztechnisch im Gastnetz und unterliegt der dortigen Sicherheits-Policy, die in den jeweiligen Einrichtungen des DFN sehr unterschiedlich ist.

Für das DFN-Roaming gibt es Richtlinien im Hinblick auf die Authentifizierungsmethode, nicht aber für die damit verbundenen Sicherheitsstufen. Dieses Problem kann umgangen werden, indem der Fremdbenutzer nach erfolgreicher Authentifizierung sofort einen Tunnel in sein Heimatnetz aufbaut. Damit unterliegt er wieder der Policy seiner Heimateinrichtung und der Datenverkehr wird von seinem Rechner bis in die Heimateinrichtung verschlüsselt.

Folgende Authentifizierungsmethoden werden vom DFN empfohlen:

- **Web-Authentifizierung**
  Nachdem der Fremdbenutzer eine drahtlose Verbindung hergestellt hat, muss er lediglich eine Internetseite öffnen, auf der er seinen Benutzernamen in der Form <benutzername>@<heimateinrichtung>eingibt (beispielsweise gibt ein Angehöriger der Universität Karlsruhe am Ort eines DFN-Roaming-Partners ein: <benutzer>@uni-karlsruhe.de). Dieses Verfahren ist allgemein von Hotspots in Hotels oder an Flughäfen bekannt. Auch wenn diese Authentifizierung in der Regel über https, also verschlüsselt erfolgt, ist der anschließende Datenverkehr durch die Luft keineswegs verschlüsselt!
- **Authentifizierung über 802.1X**
  Bei diesem Verfahren erfolgt die Authentifizierung des Fremdbenutzers direkt am Zugangspunkt. Des Weiteren können neben den herkömmlichen Benutzer-Passwort-Abfragen (übrigens im gleichen Format wie bei der Web-Authentifizierung) auch Zerti-

fikate zum Einsatz kommen. Beim 802.1X-Verfahren ist der Datenverkehr durch die Luft bis zum Access Point verschlüsselt, danach jedoch nicht mehr. Deshalb wird der Aufbau eines sicheren Tunnels in die Heimateinrichtung auch unter Einsatz des 802.1X-Authentifizierungsverfahren notwendig bleiben, ein angenehmer Nebeneffekt dabei ist, dass man nach Aufbau des Tunnels der Sicherheits-Policy der Heimateinrichtung unterliegt.

An der Universität Karlsruhe (TH) wird seit dem 1. Juni 2005 die Web-Authentifzierung angeboten. Die dafür notwendige SSID (Service Set Identifier) lautet VPN/WEB, wie vom DFN vorgegeben. Der Datenverkehr wird dabei nicht verschlüsselt. Es wird daher dringend empfohlen, nach erfolgreicher Authentifizierung einen sicheren Tunnel in die Heimateinrichtung aufzubauen. Alternativ können sichere Protokolle (https, imaps, ssh etc.) eingesetzt werden. Bis zum Ende des Jahres wird vermutlich auch eine Authentifizierung über Zertifikate und damit über 802.1X möglich sein.

Gründe für die Verzögerung dieses Verfahrens sind zum einen die Probleme mit den 802.1X-Supplikanten (Zusatzsoftware für die Wireless Clients, zum Teil kostenpflichtig) und zum anderen die verwendeten Access Points, da die Migration auf neue 802.1X-fähige Zugangspunkte auf dem Campus noch nicht vollständig beendet ist. Ferner ist der Aufbau einer globalen bundesweiten PKI (Public Key Infrastructure) auch noch nicht abgeschlossen, sodass die Nutzung aller Vorteile der 802.1X-Authentifizierungsmethoden ohnehin noch nicht gegeben wäre.

Eine aktuelle Liste aller am DFN-Roaming teilnehmenden Einrichtungen mit der jeweils dort möglichen Authentifizierungsmethode ist zu finden unter:
http://www.dfn.de/content/de/dienstleistungen/dfnroaming/roamingstandorte/index.html.
Weitere Einzelheiten zum DFN-Roaming unter:
http://www.dfn.de/content/de/dienstleistungen/dfnroaming/index.html.

Willi Fries, Tel. -6356,
E-Mail: fries@rz.uni-karlsruhe.de.

Identity Management

KIM - Karlsruher Integriertes InformationsManagement

Axel Maurer

Die Geschäftsprozesse der Universität Karlsruhe sind sehr verteilt organisiert. Die zentrale Verwaltung ist in nahezu alle administrativen Vorgänge involviert, aber auch die Verwaltungen in den Fakultäten und Instituten und weitere zentrale Einrichtungen wie das Rechenzentrum und die Universitätsbibliothek sind an einer großen Anzahl solcher Prozesse beteiligt. Die Vorgänge zwischen diesen Institutionen sind sehr verzahnt, die fehlende Transparenz führt allerdings immer wieder zu Doppelarbeiten und Verzögerungen. Auf Initiative des Rechenzentrums hat die Universitätsleitung daher das Projekt "Karlsruher Integriertes InformationsManagement", kurz "KIM" ins Leben gerufen. Das Ziel von KIM ist die konsequente Zusammenführung aller zugehörigen Dienste zu einer integrierten, ubiquitären Service-, Informations- und Wissensquelle für Forschung, Lehre, Studium, Weiterbildung und Verwaltung. Dieses Projekt wird als so innovativ betrachtet, dass sich das Ministerium für Wissenschaft, Forschung und Kunst an der Finanzierung über eine so genannte Zielvereinbarung beteiligt.

Im Rahmen von KIM werden jedoch nicht die bisherigen Verfahren und zu Grunde liegenden Systeme ausgetauscht. Die Optimierung der Zusammenarbeit aller beteiligten Einrichtungen, wie der zentralen Verwaltung, den Fakultäten, Instituten und Lehrstühlen, soll vor allem durch eine erhöhte Konsistenz der Geschäftsprozesse und eine Verkürzung der Entscheidungswege erzielt werden. Erreicht wird dies mit Hilfe

einer so genannten serviceorientierten Architektur. Diese gewährleistet, dass die für den jeweiligen Verwaltungsvorgang notwendige Information - und nur die - zum richtigen Zeitpunkt am richtigen Ort zur Verfügung steht. Durch KIM werden also nicht mehr, sondern weniger personenbezogene Daten gespeichert, denn wenn diese zum richtigen Zeitpunkt durch ein anderes System geliefert werden, ist eine Bevorratung der Daten vor Ort nicht mehr notwendig. So ist KIM nicht zuletzt ein Beitrag zum Datenschutz, da der zuständige Bearbeiter oder die zuständige Bearbeiterin immer nur die Daten erhält, die er oder sie sehen darf und die zu diesem Zeitpunkt für die Erledigung der Arbeit erforderlich sind. Vorbei sein werden damit die Zeiten, in denen man am Institut, der Unibibliothek, der zentralen Verwaltung und dem Rechenzentrum seine E-Mail-Adresse oder Telefonnummer hinterlassen musste. Solche Daten werden in Zukunft an einer Stelle gespeichert, dort gepflegt und vor unerlaubtem Zugriff geschützt.

In der Pilotphase des Projekts konnte die Fakultät für Geistes- und Sozialwissenschaften als Partner für eine Prozessanalyse gewonnen werden. Dabei wird genauestens untersucht, wann welche Information benötigt wird. Anschließend werden aus den gewonnenen Kenntnissen die Dienste definiert, welche die erforderlichen Daten liefern sollen. Diese Dienste prüfen die Berechtigung der anfordernden Person und liefern dann die zu diesem Zeitpunkt notwendige Information. Selbstverständlich werden bei der Lieferung der Daten immer Verschlüsselungsverfahren eingesetzt, so dass ein Abhören der übermittelten Daten unmöglich wird.

In der ersten Phase beschäftigt sich KIM mit den Verwaltungsprozessen der Lehrveranstaltungsplanung, des Prüfungsmanagements und der Studienassistenzsysteme. Zunächst werden die vorhandenen Systeme in diesen Bereichen mit dem Ziel betrachtet, sie in das Gesamtsystem zu integrieren. Dabei kann es sein, dass das eine System nur Dienste anderer Systeme nutzt, während andere Systeme auch Dienste zur Verfügung stellen. Konkret kann das so aussehen, dass sich das zentrale Vorlesungsverzeichnis automatisch zusätzliche Informationen aus dem kommentierten Vorlesungsverzeichnis des Instituts holt, um sie dann dem ebenfalls angeschlossenen Fakultätsserver wieder zur Verfügung zu stellen. Oder aber das Studienassistenzsystem holt sich die Daten zum Studien- und Prüfungsplan aus dem Zentralsystem, um anschließend dem Studierenden darzulegen, wo er im Studium steht und welche Studien- oder Prüfungsleistungen noch absolviert werden müssen. Dadurch wird gewährleistet, dass die Daten im Assistenzsystem immer aktuell alle Änderungen der Prüfungsordnung berücksichtigen und gleichzeitig keine Doppelarbeit geleistet wird.

Die Einbeziehung der wissenschaftlichen Kompetenz der Universität in ein Projekt der Universitätsorganisation ist einer der wichtigsten Erfolgsfaktoren für KIM. Nur so sind die Zielsetzungen zu meistern, die durchaus echte Forschungsarbeit darstellen. Gerade die Abbildung von Geschäftsprozessen auf eine serviceorientierte Architektur bei gleichzeitiger Integration vorhandener Systeme ist eine wissenschaftliche Herausforderung und gleichzeitig ein Spezialgebiet der beteiligten Lehrstühle und Forschungsgruppen.

Neben dem Rechenzentrum, der zentralen Universitätsverwaltung und der Universitätsbibliothek sind mehrere Lehrstühle der Fakultäten für Wirtschaftwissenschaften und Informatik an KIM beteiligt. Die Projektleitung liegt bei Prof. Dr. W. Juling in seiner Eigenschaft als Direktor des Rechenzentrums und Ordinarius für Informatik. Die Projektverantwortung und -steuerung erfolgt durch den CIO der Universität, Prorektor Prof. Dr. N. Henze, gemeinsam mit dem Leitungsgremium des MICK (Medien- und IV-Service-Centrum Karlsruhe) in enger Abstimmung mit dem Ausschuss für Informationsverarbeitung und -versorgung (AIV). Projektorganisation und -management wurden vom Rechenzentrum der Universität übernommen.

Weitere Informationen unter:
www.kim.uni-karlsruhe.de.

Axel Maurer, Tel. -8752,
E-Mail: maurer@kim.uni-karlsruhe.de.

Security

RZ-Test: Dateisystemverschlüsselung mit Bestcrypt

Tobias Dussa / Horst Wenske

Schutz für vertrauliche Daten auf mobilen Endgeräten

Heutzutage ist es nicht mehr ungewöhnlich, mit wichtigen oder vertraulichen Daten auf dem Notebook unterwegs zu sein. USB-Sticks oder externe Festplatten mit sensitiven Daten sind inzwischen Alltagsgegenstände. Dagegen ist es eher selten, dass diese vertraulichen Daten, die leicht verloren oder gestohlen werden können, entsprechend geschützt werden.

Das Rechenzentrum empfiehlt daher, die Dateisysteme zu verschlüsseln. Dies ist eine gängige Methode, um Daten sicher auf einer Festplatte oder anderen Medien zu speichern.

Dabei wird normalerweise eine Cyrptocontainerdatei erstellt, die mit einem Passwort geschützt, in das Dateisystem integriert beziehungsweise gemountet werden kann. Danach kann mit den Dateien im Cyrptocontainer normal gearbeitet werden, d. h. es können Dateien erstellt, kopiert und gelöscht werden. Nach einem Dismount des Cryptocontainers sind die Daten sicher im Container verschlüsselt.

Es gibt inzwischen mehrere Programme für unterschiedliche Plattformen, zum Beispiel CryptoLoop (Linux) und Truecrypt (Windows), die leider noch nicht zusammenarbeiten und teilweise auch noch nicht vollständig ausgereift sind (beispielsweise schlechte Read/Write Performance oder umständliche Integration in das Betriebssystem).

Getestet hat das RZ das kommerzielle Open Source-Programm Bestcrypt, das sowohl unter Windows als auch Linux die Möglichkeit bietet, verschlüsselte Cryptocontainer zu nutzen. Da es sich bei einem Cryptocontainer um eine gewöhnliche Datei handelt, kann diese auf jedem Datenmedium gespeichert werden.

Das Programm stammt von der finnischen Firma Jetico, die auf ihrer Webseite (www.jetico.com) die aktuellen Bestcrypt-Versionen zum 30-tägigen Testen anbietet.

Die Windows-Installation von Bestcrypt ist denkbar einfach: Es muss lediglich die Datei `bcrypt7.exe` ausführt und den Anweisungen gefolgt werden (bei einer registrierten Version wird noch der Lizenzschlüssel eingegeben.). Bestcrypt integriert sich gut in die Windows-Umgebung, da es sowohl über das Kontextmenü als auch die Taskleiste bequem aufrufbar beziehungsweise konfigurierbar ist.

Jetico bietet für die Linux-Installation RPM Packages oder Tarballs mit den jeweiligen Quellen an.

Das RZ hat auf einem Linux Debian Sarge-System (Vanilla Kernel 2.6.11) die notwendigen Kernelmodule und Programme mit einem einfachen `make && make install` gebaut und installiert (die Kernel-headerfiles müssen auf dem System installiert sein). Darüber hinaus war es bei der RZ-Installation noch erforderlich, das Verzeichnis `/var/lock/subsys` von Hand anzulegen, ansonsten hätte das Startskript sein Lockfile nicht schreiben können.

Nach dem Starten des Runlevel-Startskripts `/etc/init.d/bcrypt start` sollte der Befehl `lsmod` anzeigen, dass die Bestcrypt- und die Cryptomodule geladen wurden:

```
$ lsmod
…
bc 20584  10 bc_cast, bc_rijn, bc_idea,
bc_3des,bc_bf128, bc_bf448, bc_twofish,
bc_gost,bc_des,bc_blowfish
…
```

Danach kann mit dem Kommandozeilenprogramm `bctool` ein Cryptocontainer erstellt, gemountet werden etc. Eine nette grafische Oberfläche wird nicht angeboten, was die meisten Linuxbenutzer aber wohl nicht verschrecken wird, da `bctool` gut dokumentiert und leicht zu bedienen ist.

Bestcrypt unterstützt die gängigen Crypto- und Hashkey-Algorithmen, wobei durch ein Plugin-System die Liste der Algorithmen jederzeit erweitert werden kann (es stehen frei herunterladbare Encryption-Module zur Verfügung). Des Weiteren ermöglicht das Best-

crypt Development Kit, eigene Cyrptoalgorithmen zu implementieren und einzusetzen. In der Praxis wird man aber wahrscheinlich eher auf den SHA-256 Key Generator und RC6, Rijndael oder den Serpent Cryptoalgorithmus zurückgreifen (RC6 bietet die beste Read/Write Performance unter Bestcrypt).

Neben einem normalen Cryptocontainer kann auch ein so genannter Hidden Cryptocontainer in einem bereits bestehenden Cryptocontainer angelegt werden. Beim Erstellen eines normalen Cryptocontainers wird der gesamte Container mit Zufallsdaten aufgefüllt, die mit den eigentlichen Daten später überschrieben werden. Anzumerken ist dabei, dass Größenveränderungen des Cryptocontainers nachträglich nicht mehr möglich sind. In diesem Zufallsdatenbereich kann ein Hidden Cryptocontainer angelegt werden, der von Zufallsdaten von außen nicht unterschieden werden kann. Es gibt danach für die gleiche Cryptocontainerdatei zwei Passwörter, wobei bei der Eingabe des Hidden Cryptocontainer-Passworts der Hidden Cryptocontainer und bei der Eingabe des "normalen" Passworts die Daten des normalen Cryptocontainers gemountet werden. Mit einem Hidden Cryptocontainer muss man sehr vorsichtig umgehen. In den normalen Cryptocontainer, der den Hidden Cryptocontainer enthält, dürfen nach Erstellung des Hidden Cryptocontainers keine neuen Dateien mehr erstellt oder modifiziert werden, da ansonsten Daten vom Hidden Cryptocontainer überschrieben werden.

Darüber hinaus darf nicht das NTFS-Dateisystem für den Cryptocontainer benutzt werden (stattdessen kann zum Beispiel FAT32 verwendet werden), wenn noch ein Hidden Cryptocontainer anlegt werden soll. Das NTFS-Dateisystem erstellt seinen MBR nicht nur am Anfang sondern auch in der Mitte des Dateisystems, was wiederum Teile des Hidden Cryptocontainers überschreiben würde. Eine weitere Erfahrung mit NTFS unter Windows ist, dass ein Cryptocontainer, der intern NTFS benutzt, nicht read-only gemountet werden kann (NTFS schreibt Systemvolume-Informationen).

Die Performance-Werte von Bestcrypt auf dem RZ-Testsystem waren erfreulich. Es stand ein 1,7 GHz Intel Centrino-System mit einer 250 Gigabyte externen USB 2.0-Festplatte zur Verfügung. Unter Linux und Windows wurde eine native sequentielle Lese-/Schreib-Performance von ca. 29 Mb/s (FAT32) erreicht und mit einem Bestcrypt Cryptocontainer (basierend auf FAT32) ca. 16 Mb/s. Das sind weniger als fünfzig Prozent Nettoverlust, was für ein verschlüsseltes Dateisystem ein relativ gutes Ergebnis ist.

Bestcrypt bietet eine solide Cross Platform-Dateiverschlüsselung an und bietet viel Spielraum, das System nach eigenen Bedürfnissen anzupassen.

Mit der Verschlüsselung von Dateien oder ganzer Festplatten soll der unbefugte Zugang zu den entsprechenden Daten verhindert werden. Um dieses Ziel zuverlässig zu erreichen, ist einerseits geeignete Software - insbesondere Algorithmen und Protokolle -, andererseits aber auch angemessenes Benutzerverhalten - von der Schlüsselwahl bis zum allgemeinen Umgang mit den verschlüsselten Daten - unbedingt erforderlich. Der beste Verschlüsselungsalgorithmus hilft nichts, wenn die verwendete Software den Schlüssel offen zugänglich bei den verschlüsselten Daten speichert. Andererseits hilft eine perfekt verschlüsselte Festplatte auch nur bedingt, wenn der Benutzer ein Backup der Klartextdaten auf einem ungesicherten Medium anlegt.

Die im Folgenden angeführten Hinweise sind als Denkanstoß im Hinblick darauf zu verstehen, welche Aspekte bei der Datenverschlüsselung zu berücksichtigen sind, um zu einem sinnvollen Gesamtsystem zu gelangen.

- **Schutzwürdigkeit der Daten**
  Sind die Daten, die verschlüsselt werden sollen, wirklich schutzwürdig? Zu bedenken ist, dass im Allgemeinen das Aufbrechen einer Verschlüsselung umso leichter wird, je mehr (mit demselben Schlüssel) verschlüsselte Daten dem Angreifer zur Verfügung stehen. Auf der anderen Seite ist es auch nicht ratsam, gezielt nur "geheime" Daten zu sichern, denn dann kann der Angreifer direkt erkennen, welche Daten lohnenswerte Ziele sind und seine Resourcen gezielter einsetzen. Beispielsweise sind mobile Festplatten oder USB-Sticks stärker gefährdet als im Notebook eingebaute Festplatten, die wiederum eher in falsche Hände geraten als Festplatten in Desktop-Rechnern.

- **Schlüsselwahl und -aufbewahrung**
  Wie überall, wo Passwörter, PINs, Kennwörter und Ähnliches verwendet werden, ist es wichtig, einen Kompromiss zwischen der Komplexität der Passwortes auf der einen Seite und der Bedienerfreundlichkeit auf der anderen Seite zu finden. Es nützt wenig, wenn ein Schlüssel gewählt wird, der aus kryp-

tographischer Sicht hinreichend sicher ist, den der Anwender sich aber nicht merken kann und daher auf einen Zettel schreibt und ans Notebook klebt. Andererseits ist ein einfaches Passwort, das sich der Benutzer gut merken kann, ebenfalls ungünstig, wenn es jeder Angreifer nach zwei Minuten Ausprobieren bereits gefunden hat. Ferner ist die Gefahr nicht zu unterschätzen, das Passwort zu verlieren, wenn entsprechend fahrlässig damit umgegangen wird. Eine entsprechend sichere Software vorausgesetzt (ohne die das Verschlüsseln per se unsinnig wäre), sind sämtliche verschlüsselten Daten dann verloren!

- **Praktikabilität der Verschlüsselung**
  Es sollte darauf geachtet werden, dass die gewählte Verschlüsselung der Daten für den Benutzer mit erträglichem Aufwand verbunden ist. Ist der Schutz durch Verschlüsselung zu aufwändig, so wird der Anwender wenig geneigt sein, seine Daten tatsächlich zu verschlüsseln.

- **Ganzheitliches Sicherheitskonzept**
  Insgesamt kann eine sinnvolle Verschlüsselung nur ein Teil eines ganzen Sicherheitskonzepts sein, das sowohl den Schutz vor Angreifern (Security) als auch den Schutz vor Unfällen (Safety) umfasst. Hierzu ist beispielsweise die Sicherung der Daten auf ein externes Medium notwendig, um vor Datenverlust durch Festplattenschaden zu schützen. Dabei muss wiederum beachtet werden, daß dieses Medium entweder selber verschlüsselt ist oder nur verschlüsselte Daten gesichert werden. Zusätzlich wirken sich eventuelle Hardwareprobleme auf verschlüsselte Daten viel stärker aus: Während ein gekipptes Bit in einem Text günstigenfalls genau einen Buchstaben verändert, ist bei verschlüsselten Daten ein ganzer Verschlüsselungsblock betroffen, der bei aktuellen Algorithmen zwischen acht und sechzehn Zeichen breit ist.

Tobias Dussa, Tel. -2479,
E-Mail: dussa@rz.uni-karlsruhe.de,

Horst Wenske, Tel. -8081,
E-Mail: wenske@rz.uni-karlsruhe.de.

Institut für Angewandte Informatik und Formale Beschreibungsverfahren

Online-Klausur mit ILIAS

Roland Küstermann / Joachim Melcher / Frederic Toussaint / Detlef Seese
Institut für Angewandte Informatik und Formale Beschreibungsverfahren

Automatische Korrektur und Bewertung

Klausuren mit großen Teilnehmerzahlen sind mit hohem organisatorischem und personellem Aufwand verbunden. Durch eine Online-Klausur kann der Aufwand jedoch deutlich gesenkt werden. Dabei sind wichtige rechtliche, organisatorische und technische Aspekte zu beachten und notwendige Implementierungs- und Absicherungsmaßnahmen durchzuführen. Am Institut für Angewandte Informatik und Formale Beschreibungsverfahren wurde eine solche Rechner-Klausur in Zusammenhang mit der Programmierausbildung erfolgreich umgesetzt.

Das Institut ist unter anderem für die Programmierausbildung im Grundstudium der Studiengänge Wirtschaftsingenieurwesen und technische Volkswirtschaftslehre an der Universität Karlsruhe (TH) verantwortlich. Dazu wird jedes Wintersemester die Vorlesung “Programmieren I: Java” angeboten, die zuletzt im WS 2004/05 550 Teilnehmer hatte. Das Bestehen der abschließenden schriftlichen Klausur ist zwingender Bestandteil des Grundstudiums. Für Studierende, die die Hauptklausur nicht bestehen oder zum Beispiel wegen Krankheit nicht daran teilnehmen können, wird jeweils im darauf folgenden Sommersemester eine Wiederholungsklausur angeboten.

Die Durchführung dieser Klausuren ist - schon auf-

grund der großen Teilnehmerzahlen - mit enormem organisatorischem und personellem Aufwand verbunden, der insbesondere auch im Hinblick auf die zukünftig verfügbaren Ressourcen verringert werden soll. Die Überlegungen im Institut führten daher zu folgendem Szenario: Statt einer schriftlichen Klausur, die danach manuell korrigiert werden muss, sollte eine Klausur am Rechner durchgeführt werden, die anschließend vom Computer automatisch korrigiert und bewertet werden kann. Um den prüfungsrechtlichen Anforderungen an eine Klausur zu genügen, sollte sie entweder in Rechnerräumen der Universität oder unter Aufsicht einer Vertrauensperson stattfinden. Dort kann durch die Klausuraufsicht die Identität der Klausurteilnehmer überprüft und sichergestellt werden, dass keine unerlaubten Hilfsmittel benutzt werden und nicht abgeschrieben wird.

Als erster Testdurchlauf wurde die Nachklausur im SS 2005 gewählt. Hierfür sprach die im Vergleich zur Hauptklausur geringere Anzahl der zur Klausur zugelassen Teilnehmer (91 Studierende). So konnten zeitgleich ausreichend Rechnerplätze zur Verfügung gestellt werden.

Freitext- und Klapptafeltests

Die Programmierklausuren bestanden bisher aus einer Mischung aus Wissens- und Verständnisfragen sowie dem Schreiben bzw. Ergänzen von Programmcode. Die erstgenannten Fragen können im Rechner beispielsweise durch Multiple-Choice-, Auswahl- oder Lückentextfragen relativ einfach umgesetzt und anschließend automatisch korrigiert werden. Das automatische Überprüfen von Programmtext ist dagegen schwieriger bzw. gänzlich unmöglich. Nach wie vor sind Rechner allgemein nicht in der Lage, die Bedeutung von Programmcode zu verstehen und ihn mit dem gewünschten Verhalten zu vergleichen.

Es gibt Ansätze, die Korrektheit eines Programms durch Testen mit vorher festgelegten Testfällen, für die die gewünschten Ausgaben bekannt sind, zu überprüfen. Ein Beispiel ist das System “Praktomat”, das an der Universität Passau entwickelt wurde, um große Programmierpraktika zu unterstützen. Dieser Ansatz hat jedoch den Nachteil, dass die Korrektheit eines Programms nur bis zu einer hohen Wahrscheinlichkeit untermauert, aber nie vollständig bewiesen werden kann. Außerdem würde er nur eine Alles-oder-Nichts-Entscheidung zulassen: Entweder ist das Programm korrekt und der Studierende bekommt die volle Punktzahl oder es ist fehlerhaft und es werden überhaupt keine Punkte vergeben, obwohl es vielleicht fast richtig ist. Dies ist jedoch für eine faire Rechner-Klausur nicht erwünscht.

Aus diesem Grund hat sich das Institut für ein anderes Verfahren entschieden: Neben klassischen Single Choice-Aufgaben werden Programmieraufgaben mit Hilfe von Freitext- und Klapptafeltests realisiert. Ausgehend vom bereits vorhandenen Programmgerüst müssen an den entscheidenden Stellen, an denen das Verständnis von Konzepten abgeprüft werden soll, Lücken gelassen werden, die vom Studierenden korrekt ausgefüllt werden sollen. Damit besteht die Möglichkeit, richtige Teillösungen innerhalb einer Programmieraufgabe zu bepunkten.

Rechtliche Anforderungen

Bei der Durchführung von Klausuren müssen gewisse rechtliche Bestimmungen eingehalten werden:

- **Beweis- und Archivierungspflicht**
  Klausuren müssen mindestens fünf Jahre aufbewahrt werden, um nachträglich die Korrektheit der Notenvergabe nachweisen zu können. Im Falle einer Rechner-Klausur liegen die vom Studierenden gegebenen Antworten jedoch nur in elektronischer Form vor. Diese müssten nun über den vorgeschriebenen Zeitraum zuverlässig und nachweisbar unverändert gespeichert werden. Während die reine Speicherung technisch keine Schwierigkeit darstellt, könnte man die Unverändertheit der Daten nur mittels elektronischer Signatur sicherstellen. Da an der Universität bisher keine entsprechende technische Infrastruktur bereitsteht, würde dieser Aspekt zu unverhältnismäßig hohem Aufwand führen.

- **Datenschutz**
  Die Antworten und Noten der Studierenden dürfen Unbefugten nicht zugänglich sein. Reicht bei schriftlichen Klausuren die Einschränkung des physischen Zugangs, müssten elektronische Daten durch Verschlüsselung gesichert werden.

Um all diese Probleme zu umgehen, hat sich das Institut dafür entschieden, die Antworten der Studierenden nach Ende der Klausur auszudrucken und unterschreiben zu lassen. So erhält das Insitut trotz Rech-

ner-Klausur schriftliche Dokumente, die wie bisher archiviert werden können und deren Authentizität durch die Unterschriften der Studierenden garantiert wird. Die elektronischen Daten werden anschließend gelöscht.

Umsetzung mit ILIAS

Um eine Prüfungssituation im ILIAS-System[1] zu ermöglichen, wurde das System um den Testmodus "Online Exam" erweitert. Dieser Modus deckt eine Reihe von Anforderungen ab, welche sich zum einen in die Phasen Prüfungsvorlauf, -durchführung und -ende, zum anderen auch hinsichtlich der betroffenen Ressourcen, also den Prüfungsverantwortlichen, den Aufsichten und den Prüfungsteilnehmern, unterteilen lassen.

Im Prüfungsvorlauf muss der Prüfungsverantwortliche bei einer Reihe von Aktionen unterstützt werden. Neben den üblichen Teilnehmerdaten müssen die IP-Adressen der einzelnen Rechner bekannt sein. Für jeden Poolraum wird eine Kopie des Tests erstellt, so dass die Tests von den Aufsicht Führenden separat gestartet werden können. Für jeden Poolraum muss dann eine separate Rolle, basierend auf einer zuvor erstellten Vorlage, erzeugt werden, welcher der jeweilige Test zugeordnet wird. Die Teilnehmer werden dann beim Import diesen Rollen automatisch zugewiesen und finden somit beim Einloggen ihren Test auf dem persönlichen Schreibtisch vor. Jedem Teilnehmer wird zuvor über einen Verteilmechanismus eine IP zugewiesen, welche einer Sitzplatznummer im herkömmlichen Sinne entspricht. Bei der Zuweisung der Teilnehmer zu einem Test wird diese IP aus dem Profil übernommen. Damit hat der Studierende nur Zugang zu dem Test aus seinem Pool. Die feste Bindung einer IP an einen Nutzer ist deshalb nötig, da durch den Austausch der Benutzerdaten ein Zugriff auf den Test anderer Klausurteilnehmer erfolgen könnte.

Die Prüfungsdurchführung betrifft zum einen die Aufsicht Führenden wie auch die Prüfungsteilnehmer. Zum gewünschten Zeitpunkt wird der Test durch die Aufsicht pro Poolraum freigeschaltet. Der Status der einzelnen Tests wird überwacht. Nach Ablauf der Prüfung sind die Ergebnis- und Antwortübersichten eines jeden Studierenden druckbar. Eine Übersichtsseite erlaubt dem Prüfungsteilnehmer die freie Navigation in den Aufgaben und gibt Information zu Inhalt (Metadaten) und Gewichtung (Punkte). Die Übersicht ist von jeder Aufgabe erreichbar und gibt darüber hinaus einen Überblick über den vom Teilnehmer festgelegten Bearbeitungsstatus einer Aufgabe. Nach der finalen Abgabe der Antworten (Voransicht) öffnet sich ein neues Fenster mit der Druckansicht seiner Antworten. Ab diesem Zeitpunkt erfolgt keine Kommunikation mehr mit dem System; die Antwortenübersicht wird per Internet-Browser an einen Drucker geschickt. Die Druckansicht enthält notwendige Identifizierungsmerkmale wie IP-Adresse und Matrikelnummer auf jeder Seite und muss vom Studierenden per Unterschrift authentisiert werden.

Da die Prüfung und deren Ergebnisse aus rechtlichen Gründen fünf Jahre aufbewahrt werden müssen, werden die unterschriebenen Antwortenübersichten zusammen mit der Druckansicht der Einzelergebnisse und dem Gesamtausdruck der Klausur archiviert. Für den Reimport der Ergebnisse in bestehende Prüfungsverwaltungssysteme wurde ein Export (CSV-Format) realisiert.

Technische Anforderungen

Die Vorgabe für die Realisierung einer Online-Klausur war, dass sie an Rechnern durchgeführt werden kann, die nicht zusätzlich zeitaufwendig abgesichert werden müssen. Es sollte möglichst "auf Klick" nur für den Zeitraum der Klausurdurchführung eine sichere Umgebung geschaffen werden, ansonsten soll an den Rechnern der normale Übungsbetrieb durchgeführt werden. Die Herausforderung bestand darin, dass im Klausurszenario nicht nur Angriffe von außen abgefangen werden müssen, sondern der Studierende am Rechner keine Möglichkeit erhalten soll, über das Netz, von lokalen Rechnerressourcen oder eingelegten CDs und USB-Sticks Informationen abzugreifen. Da ILIAS eine Client-Server-Architektur voraussetzt, konnten die Rechner nicht vom Netzwerk getrennt werden.

Die vorliegende Lösung setzt auf einem Windows XP-Client mit Internet Explorer auf. Lösungen mit Mozilla als Browser oder Linux als Betriebssystem wurden ebenfalls kurz untersucht, nach Schwierigkeiten bei der Kontrolle von Zusatzfunktionen aber nicht weiter verfolgt. Weitere untersuchte Browser, die einen "Kioskmodus" unterstützen, hatten immer Lücken, die

[1] Die Open Source-Lernplattform ILIAS wird derzeit in über 600 Installationen weltweit eingesetzt. Die durchgeführten Änderungen wurden in das bevorstehende Release 3.5 mit aufgenommen. Dieses ist verfügbar unter http://www.ilias.de.

für eine Klausurumgebung nicht tolerierbar sind.

Für die Lösung eines sicheren Klausurrechners muss auf verschiedenen Ebenen angesetzt werden. Grundsätzlich muss sichergestellt sein, dass nur benötigte Programme gestartet werden können und Netzwerkverbindungen außer zum ILIAS-Server verworfen werden. Zusätzlich muss jeder Zugriff auf Konsole, Taskmanager, Taskleiste, Dialogboxen, bestimmte Tastenkombinationen und Mausfunktionen, Einstellungen zur Bildschirm-Auflösung sowie die Zoomfunktion des Systems oder die Schriftvergrößerung unterbunden werden. Als erste Maßnahme wird im schreibgeschützten Profil des Klausurbenutzers als "Shell" direkt ein Controllerprogramm gesetzt, das die "normale" Windows-Umgebung ersetzt. Das konfigurierbare Controllerprogramm IEController startet einen Internet Explorer. Es kontrolliert wichtige API-Funktionen und stellt damit sicher, dass nur vertrauenswürdige Seiten aufgerufen werden, Menüs nicht manipuliert werden können oder unbekannte COM-Objekte und externe Programme gesperrt werden. Außerdem wird der Controller automatisch im Read-Only-Modus gestartet, so dass keine weiteren Änderungen vom Anwender möglich sind.

Am Internet Explorer selbst werden alle Symbolleisten ausgeblendet bzw. die Hauptleiste so angepasst, dass nur die wichtigsten Elemente vorhanden sind. Weitere Eigenschaften, wie "Programmfenster darf nicht beendet werden", Deaktivierung des Taskmanager, Verteilung der Klausursoftware, Konfiguration von Windows-Diensten usw., werden durch Registryeingriffe und Gruppenrichtlinien überwacht. Hintergrundprogramme, die durch ein Loginskript gestartet werden, unterdrücken alle unberechtigten Tastenkombinationen (insbesondere auch Systemfunktionen im Zusammenhang mit der Windows-Taste) und Funktionen der rechten Maustaste. Das Loginskript stellt zusätzlich sicher, dass jeweils ein Drucker im aktuellen Raum verbunden und als Standarddrucker eingestellt wird. Für den Aufsichtsrechner steht ein kleines selbst geschriebenes Tool zur Verfügung, das den Remote-Neustart und den Remote-Login aller Rechner eines Pools erlaubt und ständig aktualisierte Informationen anzeigt, welcher Rechner vom Netz getrennt wurde oder wo sich ein anderer Benutzer angemeldet hat.

Viele hier aus Platzgründen nicht vorgestellte Einstellungen sind zusätzlich nötig, damit dem Benutzer keine Möglichkeit gegeben wird, auf andere als die gewünschten Ressourcen zugreifen zu können. Diese Einstellungen können aber über die gleichen oben genannten Mechanismen vorgenommen werden. Eine absolute Sicherheit ist allerdings technisch und organisatorisch nicht realisierbar.

Prüfungsdurchführung

Den Studenten wurde im Vorfeld der Klausur im vorlesungsbegleitend eingesetzten ILIAS-System eine kleine Testklausur mit typischen Aufgaben zum Kennenlernen der neuen Funktionalität bereitgestellt.

Zuvor durchgeführte Worst-Case-Lasttests mit dem Werkzeug JMeter zeigten, dass die geplante Hardwareausstattung einer Volllast nicht Stand halten würde. Daher wurde auf eine verteilte Konfiguration gesetzt. Ein leistungsstarker Server (2,8 GHz XEON, 2 GB RAM) bot den Datenbankdienst und einen Apache-Webserver als ILIAS-Host an. Zusätzlich wurden vier Desktop-Rechner (P4 3 GHz, 1 GB RAM) mit gespiegelten Installationen als ILIAS-Hosts ohne Datenbank eingesetzt. Der Zugriff der 104 Prüfungscomputer wurde über ein Startskript gleichmäßig über die fünf ILIAS-Installationen verteilt. Die tatsächliche Teilnehmerzahl betrug letztendlich 52. Über die gesamte Prüfungsdauer von 120 Minuten verlief die Prüfung reibungslos. Lastprobleme traten zu keiner Zeit auf.

Aufwand um ca. fünfzig Prozent reduziert

Um eine Rückmeldung der Teilnehmer über das neue Klausurkonzept zu erhalten, wurde eine abschließende Evaluation in Form einer Umfrage durchgeführt, deren Ergebnisse durchweg positiv im Hinblick auf Inhalt, Technik und Organisation sind. Wichtig für die Teilnehmer war insbesondere die Möglichkeit, den neuen Testmodus anhand einer Übungsklausur im Produktivsystem kennen zu lernen.

Inwiefern der Aufwand für die Rechner-Klausur geringer ist als für die schriftliche, lässt sich nur anhand einer Analyse der einzelnen Bestandteile der Klausurabwicklung bestimmen. Im vorliegenden Fall sind inhaltliche und technische Aspekte der Klausurerstellung, Druckaufsicht, Klausur- und Hörsaalvorbereitung, Klausuraufsicht, -korrektur, -ergebnisbereitstellung und -einsicht zu berücksichtigen. Basierend auf Erfahrungswerten ergab die Analyse dieser Bestandteile für eine schriftliche Klausur einen fixen Aufwand von 21 Mannstunden (Mh) gegenüber 25,5 Mh bei einer ILIAS-Klausur. Maßgeblich für den Gesamtaufwand

ist jedoch vor allem der variable Anteil. Dieser beläuft sich auf 0,59 Mh/Studierender bzw. 0,27 Mh/Studierender. Der entfallende manuelle Korrekturaufwand ist ausschlaggebend für diesen Unterschied. Bei 52 Teilnehmern stünden 51,7 Mh gegenüber 39,5 Mh bei der Rechner-Klausur. Bei großer Teilnehmerzahl lässt sich unter Vernachlässigung des fixen Anteils der Aufwand um ca. fünfzig Prozent reduzieren. Auch wenn sich ein solches Einsparungspotenzial nicht auf alle Anwendungsdomänen übertragen lässt, ist die Durchführung einer Rechnerprüfung mit ILIAS sowohl inhaltlich und rechtlich als auch technisch und organisatorisch möglich.

Änderungen bei der Vergabe von Web-Aliasen

Ulrich Weiß

Keine server- bzw. domainübergreifenden Aliase mehr

Mit Web-Aliasen, d. h. Webadressen mit einer Tilde und anschließendem Namen im Dokumentenpfad, können längere Webadressen, die man sich nicht so einfach merken kann, abgekürzt werden. Außerdem bieten diese Adressen - zum Beispiel www.rz.uni-karlsruhe.de/~stud/ mit der Endung "~stud" - die Möglichkeit von accountunabhängigen Adressen. Diesen Vorteil nutzen bislang vor allem Gruppen und Einrichtungen für ihre Webseiten, ohne dass sich deren URLs durch Autoren- und einen damit verbundenen Accountwechsel ändern. Für Informationsanbieter ändert sich mit der Einführung des neuen Webserver-Clusters und neuer Serverstrukturen die Handhabung dieser Adressen.

Die größte Änderung liegt darin, dass Aliase nicht mehr server- bzw. domainenübergreifend vergeben werden können. Beispielsweise kann auf diese Weise www.uni-karlsruhe.de/~stud/ nicht auf www.stud.uni-karlsruhe.de/ verweisen. Für Informationssuchende wird durch diese Vorgehensweise vor allem die Herkunft der Daten und die zugehörige inhaltliche Verantwortung deutlich.

Web-Aliase auf den Servern www.rz.uni-karlsruhe.de bzw. www.stud.uni-karlsruhe.de können nur für RZ- bzw. Studierenden-Accounts vergeben werden. Die Aliase für Einrichtungen, Hochschulgruppen oder studentische Gruppen können sowohl über einen RZ-Account als auch über einen Studierenden-Account angelegt werden.

Persönliche Aliase

Für RZ-Accounts, d. h. Accounts für Universitätsmitglieder, wird beim Anlegen einer eigenen Webseite standardmäßig www.rz.uni-karlsruhe.de/~<rz-account>/ angelegt. Die zugehörigen Webseiten müssen dazu im Filesystem im Pfad `~/.public_html/` des entsprechenden Accounts abgelegt werden (detaillierte Anleitungen finden Sie unter dem RZ-Softlink 50701). Zusätzlich wird zu dem kryptischen Accountnamen der Alias "~<Vorname.Nachname>" eingerichtet. Für Studierenden-Accounts wird nach dem Anlegen einer Webseite standardmäßig www.stud.uni-karlsruhe.de/~<stud-account>/ bzw. "~<Vorname.Nachname>" eingerichtet.

Gruppenaliase

Generell können auf der Homepage eines Accounts nur persönliche Aliase eingerichtet werden, die den Besitzer betreffen. Wenn unter dem Account Informationen für Gruppen angeboten werden, so können Gruppen-Aliase verwendet werden. Diese spezifizieren nicht die persönliche Homepage, sondern führen zu den Webseiten einer Gruppe bzw. Einrichtung. Die zugehörigen Informationen müssen dazu in einem gleichlautenden Verzeichnis abgelegt werden. Beispiel: Die zum Alias "~fg5" gehörenden Seiten müssen im Filesystem des Autors unter `~/.public_html/fg5/` abgelegt werden. Verzeichnisstrukturen, die nicht direkt unterhalb des Verzeichnisses `~/.public_html/` beginnen, können mit Aliasen nicht abgekürzt werden.

Alle Web-Aliase, die keine User-Aliase sind, also nicht über einen RZ- oder einen Studierenden-Account laufen, werden zum Jahresende gelöscht. Dies gilt auch für Gruppen-Aliase, die nicht auf gleichlautende Verzeichnisse verweisen. Es können keine neuen Aliase

domainenübergreifend eingerichtet werden, des Weiteren entfallen Aliase unter www.uni-karlsruhe.de gänzlich. Die unter www.uni-karlsruhe.de bestehenden Aliase werden ebenfalls am 31.12.2005 gelöscht. Für die Einrichtung neuer Aliase wenden Sie sich bitte an das BIT8000 im Rechenzentrum.

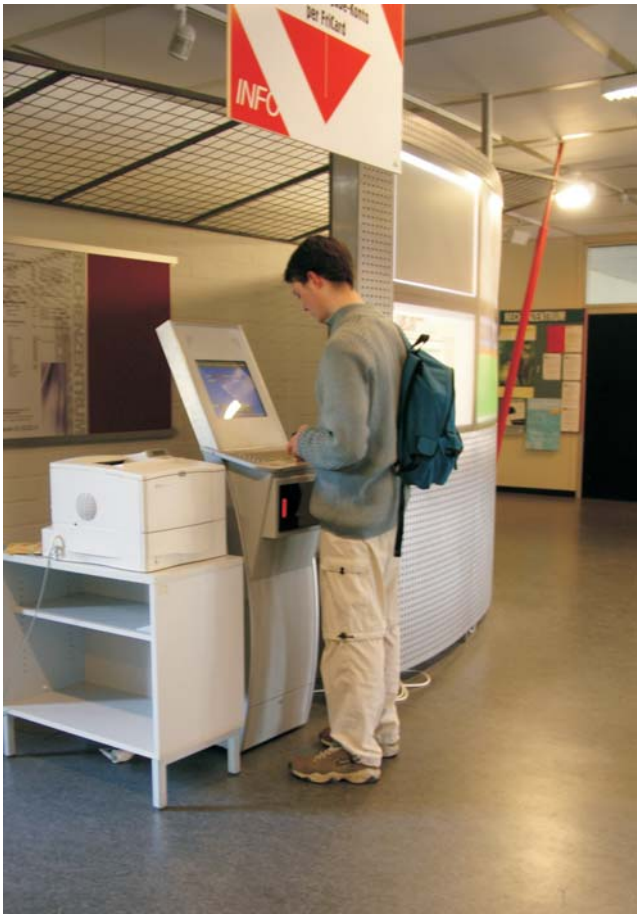
Ulrich Weiß, Tel. -4868,
E-Mail: weiss@rz.uni-karlsruhe.de.

Neu am RZ: Handbuchverkauf per Fricard

Helmut Kempermann

Nach Einführung der automatisierten Einzahlung auf das Studierenden-Druckkontingentkonto und der automatisierten Freischaltung von Studierenden-Accounts wurde nun auch der Handbuchverkauf über die FriCard realisiert.

Der Verkauf von Handbüchern des RRZN Hannover, der bis vor kurzem noch vom Studentenwerk abgewickelt wurde, wurde Anfang April 2005 vom Rechenzentrum übernommen. Mit den Möglichkeiten, welche die FriCard bietet, konnte das RZ diesen Dienst weitgehend automatisieren und vor allem aber bargeldlos realisieren. Alle, die im Besitz einer FriCard bzw. einer Mensakarte sind, können am FriCard-Terminal im Foyer des Rechenzentrums Handbücher kaufen. Welche Bücher zu welchem Preis zur Verfügung stehen, kann sowohl am Terminal als auch auf den RZ-WWW-Seiten (http://www.rz.uni-karlsruhe.de/publikationen/2817.php) eingesehen werden.



Fricard-Terminal im Foyer des Rechenzentrums.

Foto: sl

Mit Hilfe des vom Rechenzentrum entwickelten Programms kann der Fricard-Inhaber den Kauf der Handbücher weitgehend selbsttätig durchführen. Sobald ein Kauf getätigt wird, kommt die Aufforderung die FriCard (Geldkarte) in den Abwerter einzulegen, um die notwendigen Aktionen (Geldabbuchung, Eintrag in der BV, Führung der Buchungsliste) einleiten zu können. Zum Abschluss der Einkäufe wird auf dem neben dem Terminal stehenden Drucker eine Liste der erworbenen Bücher ausgedruckt. Mit dieser Liste kann dann beim BIT8000 die Ware abgeholt werden. Um Missbrauch zu verhindern, wird von den Mitarbeitern kontrolliert, ob diese Bücher auch tatsächlich gekauft und noch nicht abgeholt wurden.

Der Verkauf erfolgt ausschließlich an Studierende und Mitarbeiter/-innen der FH/TH Karlsruhe und nur zum eigenen Gebrauch.

Nicht kaufberechtigte Interessenten der Handbücher des RRZN Hannover wenden sich bitte direkt an den Herdt-Verlag: Bestell-Hotline 01801 437381, Info-Hotline 01801 437382.

Helmut Kempermann, Tel. -4038,
E-Mail: kempermann@rz.uni-karlsruhe.de.

Datenvisualisierung- und -analyse

Lizenzangebot OriginPro 7.5

Dieter Oberle

Wer beteiligt sich?

Die Datenvisualisierungs- und -analysesoftware OriginPro 7.5 mit Statistikfunktion wird derzeit als Campuslizenz "unlimited" angeboten. Dem Rechenzentrum ist bekannt, dass die Software Origin 7.5 (eingeschränkter Funktionsumfang gegenüber OriginPro) sowie ältere Versionen in verschiedenen Fachbereichen eingesetzt werden. Origin7.5 wird zurzeit in Form von Einzelplatzlizenzen und limitierten Netzwerklizenzen als Landeslizenz im Software Shop des Rechenzentrums bei der asknet AG unter https://rzunika.asknet.de/cgi-bin/product/P11442 angeboten.

Der Preis für eine Einzelplatzlizenz OriginPro 7.5 (http://shop.additive-net.de/origin) liegt bei ca. 875 Euro. Das dem Rechenzentrum vorliegende Campuslizenzangebot würde sich bei einem Stückpreis von 875 Euro bereits schon ab der 25. Einzelplatzlizenz rechnen, d. h. ab einer in der Universität verkauften Stückzahl von 25 OriginPro-Einzelplatzlizenzen würde sich der Preis schon reduzieren. Die Campuslizenz wird mit dem bekannten Lizenzmanager FlexLM betrieben. Es können bis zu fünf Lizenzserver aufgebaut werden. Die Verwendung als Einzelplatzlizenz auf nicht im Netzwerk der Universität eingebundenen Computern, vorwiegend mobilen Geräten, ist möglich und enthalten.

Die Resonanz und die Rückmeldungen zu dieser auf der ITB-Versammlung am 20.06.2005 vorgestellten Thematik hat das RZ veranlasst, an dieser Stelle noch einmal über die neue Möglichkeit zu informieren und bei Interesse eine schnelle Rückmeldung zu erbitten.

Das RZ geht in erster Näherung davon aus, dass sich der Preis pro Lizenz zwischen 400 und 500 Euro einpendeln wird. Doch es gilt, je mehr Interessenten, desto günstiger der Preis!

Hier noch einmal eine kurze Übersicht zu den Eigenschaften von OriginPro:

- Importmöglichkeiten
- Grafik-Galerie
- Datenanalyse und Statistik
- Digitale Bildverarbeitung und Smith® Diagramme
- Diagramme beschriften und Objekte einzeichnen
- Präsentationen und Publikationen
- Organisieren der Arbeit
- Programmierprojekte mit Origin C und den NAG® Bibliotheken

Wer sich also beteiligen und in nächster Zeit Lizenzen beschaffen möchte, sollte sich bis zum **15.08.2005** unter Angabe der gewünschten Stückzahl an den Autor wenden.

Dieter Oberle, Tel. -2067,
E-Mail: oberle@rz.uni-karlsruhe.de.

Betriebssysteme

Apple Mac OS X 10.4 ab sofort im RZ-Sofware Shop erhältlich

Dieter Oberle

Sonderkonditionen für die Uni Karlsruhe

Mac OS X 10.4 ist ab sofort für 58 Euro im Software Shop des Rechenzentrums unter https://rzunika.asknet.de/cgi-bin/product/P10140 erhältlich.

Reges Interesse und viele Anfragen zum Bezug des neuen Betriebssystems für Apple Computer haben das RZ veranlasst, mit der Firma über günstigere Preise bei Abnahme einer größeren Stückzahl von Lizenzen zu verhandeln. Der Preis pro Lizenz konnte von 89 Euro auf 58 Euro brutto reduziert werden. Die Lizenzen können auf dem üblichen

Weg im Online Software Shop des Rechenzentrums von allen Mitgliedern der Universität Karlsruhe und deren Einrichtungen bestellt werden. Wer außerdem Datenträger benötigt, kann diese ebenfalls für 19 Euro online ordern.

Das neue Betriebssystem wird von der Firma Apple Computer folgendermaßen beschrieben: "... Mac OS X Tiger, die fünfte wichtige Mac OS X Version, zeichnet sich durch eine stabile Grundlage aus. Diese ermöglicht die Bereitstellung praktischer und innovativer Technologien, die für die Weiterentwicklung der gesamten Branche von Nutzen sind.

- 64Bit-Programme können ohne Emulationsmodus neben 32Bit-Programmen ausgeführt werden.
- Der H.264 Codec erlaubt QuickTime 7 das Rendern von Breitbild-HD und sorgt für eine gestochen scharfe Bildanzeige bei Videokonferenzen mit iChat AV.
- Tiger Core Image überzeugt mit eindrucksvollen Funktionen und hoher Leistung für erstklassige Bildqualität.
- Die UNIX Grundlage macht Mac OS X so leistungsstark, dass es die Entwicklungsplattform der Wahl für große Open-Source-Projekte ist.
- Xgrid erlaubt die Verteilung von Verarbeitungsressourcen in Form eines Supercomputer-Knotens."

"Dank innovativer, auf einer sicheren und stabilen Grundlage basierenden Technologien macht Tiger Ihren Mac zu einem perfekt abgestimmten Instrument, mit dem Sie sich ganz auf anstehende Aufgaben konzentrieren können. Dabei spielt es keine Rolle, ob Sie für Ihren iPod neue Musik fürs Fitnessstudio zusammenstellen, an einer wissenschaftlichen Arbeit über das menschliche Genom arbeiten oder die Spezialeffekte eines neuen Films optimieren. ...

Gut durchdachte Designentscheidungen auf allen Ebenen haben es den Apple Entwicklern ermöglicht, bahnbrechende Technologien wie Spotlight und Dashboard bereitzustellen, mit denen Sie von noch mehr Leistung profitieren.

Merkmale

Gesuchtes rasant schnell finden

Spotlight ist nahtlos in das gesamte System integriert und hilft Ihnen dabei, alles innerhalb kürzester Zeit zu finden. So sind Sie ohne großen Zeitaufwand perfekt organisiert.

- Suchen Sie nach Objekten aller Art mit dem systemweit verfügbaren Spotlight Menü - jederzeit.
- Finden Sie auch in umfangreichen PDF-Dateien gewünschte Informationen, ohne zusätzliche Software.
- Erstellen Sie intelligente Ordner, die nach dem Hinzufügen neuer Dateien automatisch aktualisiert werden.
- Arbeiten Sie mit intelligenten Postfächern, um Ihre E-Mails auf vielfache Weise anzuzeigen und zu ordnen.
- Steuern Sie Ihre Systemeinstellungen ohne Aufwand mit einer Suche, die die benötigte Systemeinstellung voraussagt.
- Verwenden Sie intelligente Gruppen, um Ihre Kontakte und Kategorien automatisch zu sortieren.

Überschaubarer Arbeitsbereich

Profitieren Sie von einem übersichtlichen und ordentlichen Arbeitsbereich mit Zugriff auf alles, was Sie brauchen - und zwar jederzeit. Sie haben die Kontrolle und können genau festlegen, welche Taste oder welches Menü immer verfügbar sein soll.

- Dashboard stellt praktische und nützliche Miniprogramme, so genannte Widgets bereit - und blendet
- sie aus, wenn Sie sie nicht benötigen.
- Automator nimmt Ihnen sich wiederholende Aufgaben ab, sodass Sie sie nicht selbst erledigen müssen.
- Lassen Sie sich Ihre neuen E-Mails von Ihrem Mac vorlesen. Dafür steht die neue VoiceOver Funktion zur Verfügung.
- Exposé ordnet im Handumdrehen unzählige Fenster.
- Die systemweit verfügbare Menüleiste bietet jedem Fenster mehr Platz und erlaubt den Zugriff auf Systemsteuerelemente und Hilfefunktionen.

Sicher in die Zukunft

Da Mac OS X bereits über eine sichere, zuverlässige Open-Source-Basis verfügt, können sich die Apple Techniker voll und ganz darauf konzentrieren, innovative Internet-Programme zu entwickeln, mit denen Science-Fiction für Sie schon heute zur Realität werden kann.

- Erkennen Sie auf einen Blick, wenn auf Ihren häufig besuchten Web-Sites neue Informationen verfügbar

sind, und lesen Sie diese direkt in Safari.
- Nutzen Sie eine Lösung für persönliche Videokonferenzen zum unkomplizierten Ideenaustausch mit Kollegen.
- Informieren Sie sich schnell und einfach über eine Vielzahl von Themen im Internet - vom Wetter über Börsenkurse bis hin zu Fluginformationen.
- Sorgen Sie dafür, dass alle wichtigen Informationen über mehrere Computer mit einem .Mac Account perfekt synchronisiert sind.
- Erleben Sie die Arbeit mit einem reaktionsschnellen System, das sich dank ausgeklügelter Sicherheitsmechanismen nicht durch Überwachungssoftware oder Viren lahm legen lässt.
- Stellen Sie ohne Probleme Verbindungen zu Netzwerken her - sowohl von Desktop-Computern als auch von Notebooks.

Es funktioniert einfach

Schließen Sie nahezu jedes beliebige Gerät an oder stellen Sie Verbindungen zu jedem Netzwerk her - ganz ohne Konfiguration und ohne Probleme. Der Einsatz und die Entwicklung offener Standards macht Mac OS X zur kompatibelsten Plattform, die es gibt.

- Schließen Sie unzählige Digitalkameras, Drucker, Audio- und MIDI-Geräte, DV-Camcorder, Eingabegeräte, Massenspeichergeräte und optische Medien, Scanner und Bildschirme via USB, FireWire (IEE 1394) und DVI ohne zusätzliche Software an.
- Verbinden Sie Bluetooth Geräte wie Handys und Eingabegeräte mit sicherer Verschlüsselung und synchronisieren Sie diese mit Ihrem Adressbuch und mit iCal.
- Drucken Sie via SMB-Protokoll direkt auf gemeinsam genutzten Windows-Druckern.
- Senden Sie mit dem integrierten Modem oder einem Bluetooth fähigen Handy Faxnachrichten.
- Richten Sie Geräte wie Netzwerkdrucker oder drahtlose Webcams mit der Bonjour Technologie ohne Konfiguration mühelos ein."

Sollten Sie weitere Fragen haben, wenden Sie sich bitte an Herrn Korb, Tel. -4041, E-Mail: korb@rz.uni-karlsruhe.de.

Mikroelektronik

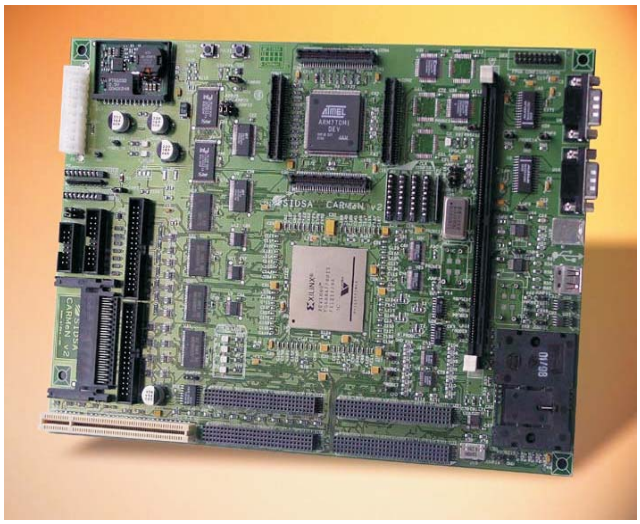
Entwicklungsplatine CARMeN zu Sonderkonditionen

Dieter Kruk

Hohe Kapazität und komfortabel

Systeme, die bisher aus diskreten Bauteilen zusammengesetzt wurden, werden jetzt oftmals auf einem einzigen Chip integriert und als SoC bezeichnet (System on Chip). Hierzu sind neuartige Entwurfsverfahren nötig, um früher insignifikante Probleme, wie Bus-Strukturen, Modellierung einer Test-Anordnung oder die Fähigkeit, in kurzer Zeit die Funktionsweise verschiedener Konfigurationen darzustellen und auszutesten, lösen zu können.

Die über EUROPRACTICE angebotene Entwicklungsplatine CARMeN (Core ARM emulatioN for Embedded SoC and Software Co-Development)



Entwicklungsplatine CARMeN

Foto: EUROPRACTICE

basiert auf der ARM®-Technologie für eingebettete Systeme und ist entweder mit einem Baustein XILINX Virtex XCV2000E oder mit einem ALTERA Apex 20k1000 bestückt. Beide FPGAs zeichnen sich durch hohe Kapazität (das Äquivalent sind 3,0 Millionen ASIC-Gatter) sowie eine beträchtliche Anzahl physikalischer Anschlüsse aus.

Zur Programmierung werden die Entwicklungswerkzeuge XILINX Alliance oder ALTERA Quartus empfohlen, die ebenfalls über die EU-Ausbildungsinitiative EUROPRACTICE erhältlich und in mehreren Instituten bereits vorhanden sind.

Die Plattform CARMeN ist komfortabel ausgestattet und bietet dem Entwickler auch Anschlussmöglichkeiten wie PCMCIA, Smart Card, PCI, ARM-JTAG-Bus, CAN Bus und USB; diese können per Software auf beliebige Außenanschlüsse gelegt werden (”soft-routable”).

Das Gerät wird in erheblichem Umfang auch industriell für SoC Hardware-/Software-Co-Entwicklungen eingesetzt. Eine begrenzte Anzahl dieser Plattformen ist jetzt für europäische Hochschulen zu vergleichsweise günstigen Bedingungen erhältlich.

Informationen und Material über die Entwicklungsplatine CARMeN erhalten Sie im Rechenzentrum. Darüber hinaus sind folgende Entwicklungstools vorhanden oder beziehbar: CADENCE, SYNOPSYS (ASIC-Entwurf), CoWare Lisatek (Hw-/Sw-Co-Entwicklung) sowie MENTOR GRAPHICS FPGA & Board Design (überwiegend verwendet zur Entwicklung von Hochleistungsplatinen). Einzelne dieser Softwarelizenzen können auch kurzfristig bereitgestellt werden; sie sind flexibel (FLEXlm) über das Netz ansprechbar.

Dieter Kruk, Tel. -3785,
E-Mail: kruk@rz.uni-karlsruhe.de.

Aristo-Zeichentisch außer Betrieb

Helmut Kempermann

Wegen der im Laufe der letzten Jahre zurückgegangenen Nachfrage seitens der Benutzer wurde der Aristo-Zeichentisch am 25. Juli 2005 außer Betrieb genommen. Damit endet nach 30 Jahren die Ausgabe von bearbeiteter Gravierfolie und Schneidefolie am RZ.

Textverarbeitung

Einführungskurs LaTeX

Dr. Klaus Braune

LaTeX ist ein Makropaket zu TeX, mit dessen Hilfe auf relativ einfache Weise Dokumente mit umfangreichen mathematischen Formeln, Abbildungen und Querverweisen erstellt werden können.

In der Zeit vom 05.09. bis 09.09.2005 findet ein Einführungskurs in LaTeX statt. Ziel des Kurses ist es, LaTeX kennenzulernen und das Erstellen von Texten mit Hilfe von LaTeX zu erlernen. Die Übungen zum Kurs finden unter Windows XP oder Linux unter Verwendung einer für LaTeX geeigneten Entwicklungsumgebung statt. Für die Teilnahme am Kurs sind keine Vorkenntnisse erforderlich. Die im Kurs erworbenen Kenntnisse können bei der Textverarbeitung an PCs ebenso angewendet werden wie auf Workstations oder Großrechnern.

Kursbeginn:	Montag, 05.09.2005, 09.00 Uhr
Ort:	RZ, Raum 217, 2. OG
	Übungen im Raum 114, 1. OG
Kursende:	Freitag, 09.09.2005, 17.00 Uhr
Anmeldung:	beim BIT8000, EG

Themen:

- Allgemeine Informationen über TeX und LaTeX
- Genereller Aufbau und Gliederung eines Dokumentes

- Die vordefinierten Dokumenttypen und Änderungen des Layouts
- Standardschriften und die Verwendung zusätzlicher Schriften
- Silbentrennung, Umlaute und scharfes S
- Listen, Tabellen, Zitate, Fußnoten
- Einfache Grafiken
- Inhaltsverzeichnis, Literaturverzeichnis und weitere Verzeichnisse
- Setzen mathematischer Formeln.

Die Teilnehmerzahl ist auf 30 begrenzt. Zur Anmeldung liegen vorbereitete Listen im BIT 8000 im EG des RZ aus (Tel. -8000, E-Mail: bit8000@rz.uni-karlsruhe.de).

Weitere Informationen zu TeX und zum LaTeX-Kurs finden Sie im WWW unter http://www.rz.uni-karlsruhe.de/~rz32/tex.html.

Literatur:

H. Kopka: LaTeX.
Band 1: Einführung, Addison Wesley Deutschland, 1994, ISBN 3-89319-664-1
Band 2: Ergänzungen, Addison Wesley Deutschland, 1994, ISBN 3-89319-665-x
L. Lamport: The LaTeX Document Preparation System, 2. Auflage, AddisonWesley USA, 1994, ISBN 0-201-52983-1
H. Partl, E. Schlegl, I. Hyna: LaTeX-Kurzbeschreibung, im Rahmen der verschiedenen TeX-Installationen als LaTeX-Datei verfügbar.

Dr. Klaus Braune, Tel. -4031,
E-Mail: braune@rz.uni-karlsruhe.de.

Statistik

Einführungskurs SAS

Dr. Klaus Braune

Der nächste SAS-Einführungskurs (Statistical Analysis System) findet vom 19.09. bis 23.09.2005 statt. Ziel des Kurses ist das Kennenlernen und Anwenden von SAS. Vorkenntnisse sind für die Kursteilnahme nicht erforderlich. Die erworbenen Kenntnisse können an Workstations oder PCs eingesetzt werden. Die statistischen Grundlagen sind nicht Lehrstoff des Kurses.

Kursbeginn:	Montag, 19.09.2005, 09.00 Uhr
Ort:	RZ, Raum 217, 2. OG Übungen im Raum 114, 1. OG
Kursende:	Freitag, 23.09.2005, 17.00 Uhr
Anmeldung:	beim BIT8000, EG

Programm:

Montag 19.09.2005

09.00 - 9.45	Überblick über Statistikprogramme am Rechenzentrum, Vorstellung von SAS
10.00 - 12.00	Die interaktive Oberfläche von SAS, der SAS-Editor, Literatur
14.00 - 15.00	Aufbau von SAS-Programmen, Variablen, Daten, Dateien
15.00 - 17.00	Betreute Übung

Dienstag 20.09.2005

09.00 - 10.30	Eingabe von Daten in SAS
10.30 - 12.00	Betreute Übung
14.00 - 15.00	Ausgabe und einfache Auswertungen von Daten
15.00 - 17.00	Betreute Übung

Mittwoch 21.09.2005

09.00 - 10.15	Interaktive Dateneingabe, Maskenerstellung (SAS/FSP)
10.15 - 12.00	Betreute Übung
14.00 - 15.30	Grafische Darstellung von Daten (SAS/GRAPH) I
15.30 - 17.00	Betreute Übung

Donnerstag 22.9.2005

09.00 - 10.30	Grafische Darstellung von Daten (SAS/GRAPH) II
10.30 - 12.00	Betreute Übung
14.00 - 15.00	Statistische Prozeduren - Überblick und Beispiel (SAS/STAT)
15.00 - 17.00	Betreute Übung

Freitag 23.9.2005

09.00 - 10.15	Überblick: SAS/ETS (Zeitreihenanalyse) SAS/OR (Operations Research) SAS/IML (Interactive Matrix Language) SAS/AF (Programmierung von Menü-Oberflächen)
10.15 - 12.00	Betreute Übung
14.00 - 15.00	Zusammenfassung der Kursinhalte, Fragen, Abschlussdiskussion
ab 15.00	Betreute Übung

An den Übungen können nur Angehörige von Hochschulen des Landes Baden-Württemberg teilnehmen.

Der Kurs findet im Raum 217, die Übungen im Raum 114 des Rechenzentrums statt (unter Linux). Die Teilnehmerzahl ist auf 20 begrenzt. Zur Anmeldung liegen vorbereitete Listen im BIT 8000 im Foyer des Rechenzentrums aus (Tel. -8000, E-Mail: bit8000@rz.uni-karlsruhe.de).

Weitere Informationen zu SAS und zum SAS-Kurs finden Sie im WWW unter http://www.rz.uni-karlsruhe.de/~rz32/sas.html).

Literatur:

SAS Version 6 - Eine Einführung mit Beispielen. Skript zum Kurs.

SAS-Anwenderhandbuch im Netz. Im WWW verfügbar unter http://www.urz.uni-heidelberg.de/statistik/sas-ah/.

Dr. Klaus Braune, Tel. -4031,
E-Mail: braune@rz.uni-karlsruhe.de.

Erste Ansprechpartner
auf einen Blick

So erreichen Sie uns

Telefonvorwahl:	+49 721/608-
Fax:	+49 721/32550
E-Mail:	Vorname.Nachname@rz.uni-karlsruhe.de

Help Desk BIT8000	Tel. -8000, E-Mail: bit8000@rz.uni-karlsruhe.de
Sekretariat	Tel. -3754, E-Mail: rz@uni-karlsruhe.de
Information	Tel. -4865, E-Mail: info@rz.uni-karlsruhe.de
PC-Beratung MicroBIT	Tel. -2997, E-Mail: microbit@rz.uni-karlsruhe.de
Scientific Supercomputing Center Karlsruhe (SSCK)	Tel. -8011, E-Mail: ssck@rz.uni-karlsruhe.de
Anwendungen	Tel. -4031/-4035, E-Mail: anwendung@rz.uni-karlsruhe.de
Netze	Tel. -6356/-7395, E-Mail: netze@rz.uni-karlsruhe.de
UNIX	Tel. -4039/-6341, E-Mail: unix@rz.uni-karlsruhe.de
Virus-Zentrum	Tel. 0721/9620122, E-Mail: virus@rz.uni-karlsruhe.de
Mailingliste für Internetmissbrauch	abuse@uni-karlsruhe.de
asknet AG (SW-Lizenzen)	Tel. 0721/964580, E-Mail: info@asknet.de
Zertifizierungsstelle (CA)	Tel. -7705, E-Mail: ca@uni-karlsruhe.de
PGP-Fingerprint	pub 1024/A70087D1 1999/01/21 CA Universität Karlsruhe 7A 27 96 52 D9 A8 C4 D4 36 B7 32 32 46 59 F5 BE

Öffentliche Rechnerzugänge

World Wide Web:

http://www.rz.uni-karlsruhe.de/(Informationssystem des Rechenzentrums der Universität Karlsruhe)

http://www.rz.uni-karlsruhe.de/ssc/ (Scientific Supercomputing Center Karlsruhe)

Ftp:

ftp.rz.uni-karlsruhe.de; Benutzernummer: ftp (anonymer Ftp-Server des Rechenzentrums)