

news

Neue Campuslizenz

Insure++ für sichere C- und C++-Programme

Effiziente Programmentwicklung

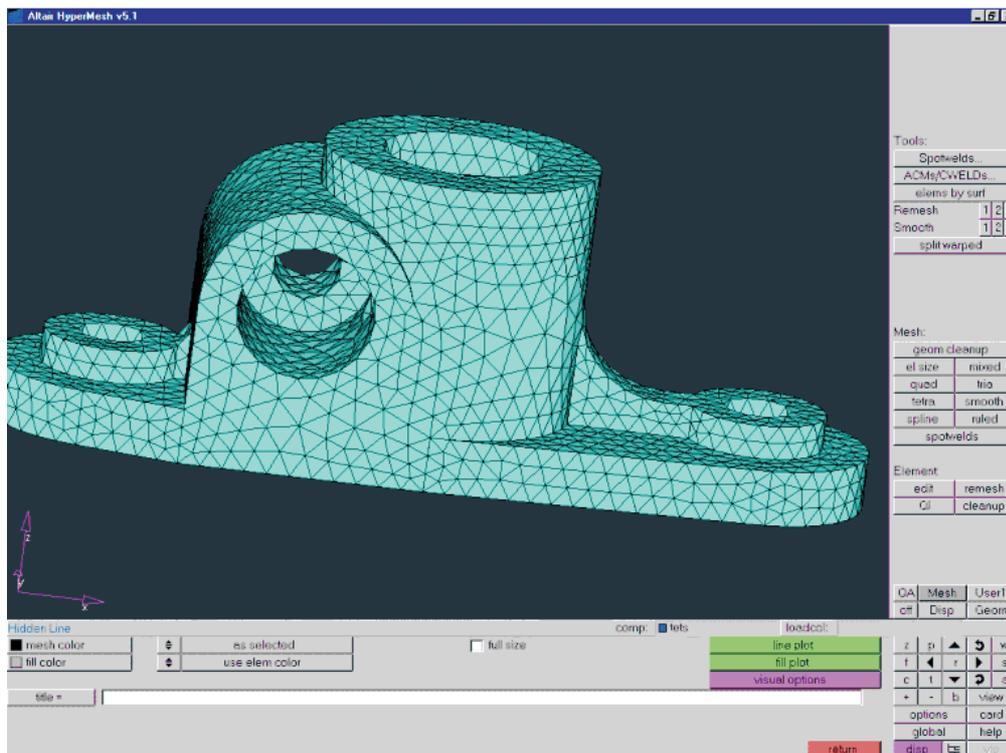
NAG Parallel Libraries

Neues Werkzeug für Finite Elemente

CAE-Umgebung Altair Hyperworks 5.1

labview

computer und
recht



Mit Hypermesh modelliertes und vernetztes Bauteil zur Berechnung mit einem FE-Programm

INHALT

Neue Campuslizenz Insure++ für sichere C- und C++-Programme	
Komfortables Tool zur Fehlerbeseitigung.	3
Messdatenverarbeitung/Anlagensteuerung LabVIEW 6.1 ist da	
Neue Funktionen	4
Neues Werkzeug für Finite Elemente Die CAE-Umgebung Altair HyperWorks 5.1	
.	5
Effiziente Programmentwicklung NAG Parallel Libraries	
Informationsveranstaltung am 4.12.2002	6
Computer und Recht Der Kopierschutz nach Änderung des Urheberrechts	
Vorbemerkung.	7
Schutz technischer Maßnahmen	8
Straf- und Bußgeldnormen	9
Personalia	
.	10
Vorträge, Workshops und Kurse auf einen Blick	
.	11
Erste Ansprechpartner auf einen Blick	
.	12

IMPRESSUM

Herausgeber:
Prof. Dr. Wilfried Juling
Redaktion: Ursula Scheller,
Klaus Hardardt
Tel.: 0721/608-4865 oder -7391

Universität Karlsruhe (TH)
Rechenzentrum
D-76128 Karlsruhe
<http://www.uni-karlsruhe.de/~RZ-News/>
Nummer 2002/9, 10
ISSN 1432-7015

Neue Campuslizenz

Insure++ für sichere C- und C++-Programme

Dr. Rudolf Lohner

Komfortables Tool zur Fehlerbeseitigung

Segmentation Violation, Bus Error, Probleme mit Pointern, Strings und Speicherverwaltung: In welchem C oder C++ Projekt kommt es nicht immer wieder zu oft sehr entnervenden und zeitraubenden Fehlersituationen?

Die großzügigen Freiheiten, die C und C++ beim Programmieren bieten, rächen sich oft mit äußerst subtilen Fehlern, denen man nur schwer auf die Spur kommt. Nicht selten bleiben diese unentdeckt und führen zu unerklärlichem Verhalten der Programme, von manchen ärgerlichen Macken bis hin zum vollständigen Crash. Die berüchtigten Buffer Overflows tragen bekanntermaßen immer wieder zur Verbreitung von Viren bei und öffnen zum Teil sehr bedenkliche Sicherheitslücken in mancher Server- und Clientsoftware.

Das Rechenzentrum bietet nun mit einer neuen Campuslizenz für die Software Insure++ von ParaSoft (<http://www.parasoft.com>) ein wirkungsvolles Tool an, mit dem man den meisten dieser Fehler sehr effizient auf die Spur kommen kann. Unter Linux mit einer glibc ab Version 2.1 steht allen Universitätsangehörigen seit September 2002 eine 'Floating License' für bis zu vier gleichzeitige Benutzer für Anwendungen ausschließlich im Bereich Lehre und Forschung zur Verfügung. Die Lizenz beinhaltet auch einen einjährigen, vollständigen Support inklusive aller Updates.

Im Gegensatz zu ähnlichen Tools, die direkt auf den übersetzten Objektcode angewandt werden, arbeitet Insure++ bereits mit dem Sourcecode der Programme: Vor dem Übersetzen baut Insure++ eine Fülle von zusätzlichen Instruktionen in den Programmtext ein, die es zur Laufzeit ermöglichen, wesentlich mehr Fehlersituationen zu erkennen, als dies bei der reinen Objektcode-Methode der Fall ist. Diese Sourcecode-Instrumentierung ist völlig transparent und bei der Benutzung von Insure++ nicht sichtbar.

Die Fehler, die von Insure++ erkannt werden, umfassen unter anderem:

- Ungewolltes Überschreiben von Speicherbereichen.
- Falsche Verwendung von Pointern: Null Pointer, uninitialisierte Pointer, ungültig gewordene Pointer, ungültige Pointervergleiche, Funktionsaufrufe über ungültige Funktionspointer.
- Speicherleichen: Identifizierung von nicht mehr erreichbarem Speicher.
- Falsche Handhabung dynamischer Speicherverwaltung (malloc/free, new/delete).
- Verwendung nicht initialisierter Speicherbereiche.
- Falsches Stringhandling.
- Fehler bei Datenkonversionen (z. B. wenn die Größe eines Pointers nicht die von int ist).
- Inkompatible Deklaration von Variablen in verschiedenen Files.
- I/O-Fehler wie z. B. falsche Formate in printf/scanf oder zu kleine Puffer.

Die Benutzung von Insure++ ist sehr komfortabel. Das Programm wird wie üblich übersetzt, wobei der Name des Compilers durch 'insure' ersetzt wird. Bei der Programmausführung wird dann ein Fenster geöffnet, in dem die Analyse von Insure++ während der Laufzeit erscheint. Durch Anklicken einer Fehlermeldung können weitere Fenster geöffnet werden, in denen der Quelltext im Editor erscheint und bereits auf die fehlerhafte Stelle positioniert ist. Welche Arten von Fehler erkannt werden sollen, wie ausführlich der Fehlerreport sein soll, wo der Fehlerreport erscheinen soll (Fenster oder einfach nur Textdatei) und viele andere Einstellungen lassen sich frei konfigurieren, so dass in jeder Situation und für jeden Geschmack die optimalen Präferenzen gewählt werden können.

Am besten probieren Sie das Tool gleich einmal aus. Da bei der Installation von Insure++ bereits eingestellt werden muss, welche C/C++ Compiler verwendet werden sollen, muss es lokal auf Ihrem Rechner installiert sein. Holen Sie sich hierzu die Datei `ins++.linux2.tar.gz` entweder von <http://www.rz.uni-karlsruhe.de/Uni/RZ/Software/Anwendungen/LANG/>

CC++ TOOLS/ oder direkt von Parasoft (-> Downloads, achten Sie auf die Version 5.2 für die Architektur Linux2).

Kopieren Sie dann diese Datei in das Verzeichnis, in dem Sie Insure++ installieren möchten und rufen Sie dort das Kommando `tar xvzf ins++.linux2.tar.gz install README Release.Notes FAQ.txt` auf. Lesen Sie die Datei README und installieren Sie dann Insure++ mit `./install`. Am Ende der Installation verneinen Sie die Frage nach dem Einrichten einer Lizenz. Statt dessen tragen Sie in die von der Installation angelegte Datei `.psrc` am Ende folgende drei Zeilen ein:

```
LicenseServer.host nz20
LicenseServer.port 2002
Registertool LicenseServer 1.0
```

Damit erhalten Sie von den Rechnern innerhalb des Campusnetzes eine Lizenz vom zentralen License Ser-

ver, wenn Sie Insure++ aufrufen. Eine ausführliche Dokumentation finden Sie nach der Installation im Unterverzeichnis `manuals` Ihres Installationsverzeichnis.

Sollten Sie Fragen oder zu Insure++ haben oder Unterstützung benötigen, wenden Sie sich bitte an den zuständigen Betreuer im Rechenzentrum (siehe unten).

Installation, Handhabung und Möglichkeiten von Insure++ werden im Rahmen des nächsten Treffens des Arbeitskreises Linux Cluster an der Universität Karlsruhe vorgestellt werden. Diese Veranstaltung findet am Mittwoch, den 13.11.2002, um 14.00 Uhr im Seminarraum 217 im Rechenzentrum statt. Alle interessierten Uni-Angehörige sind hierzu sehr herzlich eingeladen.

Dr. Rudolf Lohner, Tel. -6958,
E-Mail: Rudolf.Lohner@rz.uni-karlsruhe.de.

Messdatenverarbeitung/Anlagensteuerung

LabVIEW 6.1 ist da

Dieter Kruk

Neue Funktionen

Datenfernverarbeitung über das Internet war bereits mit LabVIEW 6.0 möglich. Mit LabVIEW 6.1 gibt es nun ein bedienungsfreundliches Werkzeug für die Erstellung von Anwendungen, die sich mittels Standard-Web-Browsern steuern lassen. Zudem weist es die neuesten Technologien für die Kommunikation mit XML und die drahtlose Datenübertragung auf. In der neuen Version stehen auch Funktionen zur erweiterten Messwertanalyse zur Verfügung, sowie Module für Echtzeit-Anwendungen, Prozessüberwachung und Datenarchivierung.

Im Rahmen der vorhandenen LabVIEW-Campuslizenz, an der sich inzwischen 33 Institute beteiligt haben, wird die neue Version auf Wunsch (gegen Kostenbeteiligung) an interessierte Institute abgegeben. Auch bei der Beschaffung von Dokumentation ist das Rechenzentrum behilflich; einzelne Handbücher sind noch vorrätig. Außerdem sind die beiden gut ausge-

statteten Standardwerke, das LabVIEW-Grundlagenbuch und -Anwenderbuch (jeweils 400 Seiten, reichhaltig illustriert, Mitverfasser in beiden Fällen: Rahman Jamal) vorhanden, die befristet an interessierte Institute ausgeliehen werden.

An dieser Stelle sei auch auf das Blockpraktikum hingewiesen, das zweimal jährlich vom Institut für Thermische Strömungsmaschinen (ITS) angeboten wird und als Programmier-Werkzeug LabVIEW verwendet. Die Teilnehmerzahl ist jeweils begrenzt, es empfiehlt sich daher eine frühzeitige Anmeldung. Näheres hierzu finden Sie auf den Web-Seiten des ITS unter Blockpraktikum.

Ein Treffen der LabVIEW-Anwender an der Uni Karlsruhe findet am Donnerstag, 24.10.2002, im Rechenzentrum statt. Einzelheiten finden Sie unter der Rubrik *Vorträge, Workshops und Kurse*. Die vorgesehene Themenliste des Treffens wird über die E-Mail-Verteilerliste *LABVIEW-L* bekannt gegeben, in die neue Interessenten auf Wunsch gerne aufgenommen werden.

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

Neues Werkzeug für Finite Elemente

Die CAE-Umgebung Altair HyperWorks 5.1

*Dr. Matthias Gölke / Altair Engineering GmbH
Dr. Paul Weber*

Altair Engineering ist eines der führenden Unternehmen im Bereich Computer Aided Engineering. Die von Altair Engineering unter dem Oberbegriff HyperWorks angebotenen Softwarelösungen im Finite-Elemente-Umfeld umfassen das Pre/Postprocessing, die Strukturoptimierung und die Simulation.

Kern von HyperWorks ist ein intelligentes Lizenzierungssystem, welches flexiblen Zugriff auf die unterschiedlichen Produkte ohne zusätzliche Kosten erlaubt.

Das Rechenzentrum hat daher eine Lizenz für dieses CAE-System erworben. HyperWorks läuft unter den gängigen UNIX-Systemen und Windows/95/98/NT/2000 und wird in den nächsten Wochen über die kleine Baumschule bereitgestellt werden. Interessenten an einer lokalen Installation auf einer Institutsmaschine wenden sich bitte an den Betreuer (siehe unten).

Die verschiedenen Softwarelösungen von HyperWorks stellen sich im Einzelnen folgendermaßen dar:

HyperMesh

Bei HyperMesh handelt es sich um einen universellen Prä- und Postprozessor für Vernetzung, Aufbau und Auswertung von Berechnungsmodellen beispielsweise für ABAQUS, ANSYS, NASTRAN oder LS-DYNA. Aufgrund seiner Funktionalität ist HyperMesh für komplexe Berechnungsaufgaben hervorragend geeignet.

HyperGraph

HyperGraph ist eine Software zur Darstellung von xy-Daten aus der technischen Berechnung und dem Versuch. Die Software stellt über 130 mathematische Auswertefunktionen zur Verfügung. Es existieren umfangreiche Manipulationsmöglichkeiten, um das gewünschte Plot-Layout zu generieren.

HyperView

Bei HyperView handelt es sich um einen FEM- und MKS-Postprozessor, der auch bei grossen Modellen hohe Animationsgeschwindigkeiten erreicht. Durch

ein „Multi-Window-Layout“ lassen sich beliebige Darstellungen erzeugen. Ergebnisse können aus allen gängigen FEM- und MKS-Paketen eingelesen und visualisiert werden.

MotionView

MotionView ist eine Umgebung zur Simulation von Mehrkörpersystemen. Mit MotionView können Ergebnisse aus ADAMS oder SIMPACK visualisiert oder mittels des eigenständigen MKS-Solvers Kinematikberechnungen sehr einfach durchgeführt werden.

OptiStruct

OptiStruct ist ein leistungsfähiges Werkzeug zur Analyse und Optimierung von Bauteilen. Verschiedene Optimierungsdisziplinen sind verfügbar: Topologie-, Topographie (Sicken-), Form- und Parameteroptimierung.

StudyWizard

Der StudyWizard stellt solverunabhängige Optimierungsroutinen zur Verfügung. So können beispielsweise Parameteroptimierungen mit ABAQUS, aber auch jedem anderen beliebigen Solver durchgeführt werden. Es steht ein sequentielles Response-Surface-Verfahren zur Verfügung. Dieses liefert insbesondere bei hochgradig nichtlinearen Problemstellungen zuverlässige Optima.

HyperForm

Bei HyperForm handelt es sich um eine Software zur Simulation von Tiefziehprozessen. Das verwendete Einschnittverfahren liefert dabei in sehr kurzer Zeit Aussagen über Ziehbarkeit, Faltenbildung und Ausdünnung von Blechteilen beim Tiefziehen. Zusätzlich bietet HyperForm eine speziell für die Tiefziehsimulation entwickelte LS-DYNA-Schnittstelle (HyperForm Incremental).

Veranstaltungshinweis

Zu HyperWorks veranstaltet die Firma Altair einen Informationstag im Rechenzentrum. Das Programm umfasst die folgenden Themen:

- Firmenpräsentation

- HyperWorks und Lizenzierung
- HyperMesh (Prä- und Postprocessing)
- HyperView und HyperViewPlayer (Postprocessing)
- Optimieren mit OptiStruct
- Tiefziehen mit HyperForm (OneStep)

Datum: 8. November 2002

Zeit: 9.00 - ca. 12.00 Uhr

Ort: RZ, Raum 217, 2. OG

Um einen Überblick über die Anzahl der Teilnehmer

zu erhalten, bitte eine kurze Mitteilung per E-Mail oder Telefon an:

Dr. Paul Weber, Tel. -4035,

E-Mail: weber@rz.uni-karlsruhe.de.

Hersteller:

Altair Engineering GmbH / Böblingen

Tel.: +49-(0)7031-6208-0

Fax : +49-(0)7031-6208-99

<http://www.altair.de>.

Effiziente Programmentwicklung NAG Parallel Libraries

Nikolaus Geers

Informationsveranstaltung am 4. 12. 2002

Die Unterprogrammbibliotheken der Numerical Algorithms Group sind seit vielen Jahren in der Universität Karlsruhe im Einsatz. Diese Bibliotheken decken einen großen Bereich der Numerik und Statistik ab und sind auf einer Vielzahl von Rechnerplattformen verfügbar. Im Rahmen einer Landeslizenz stehen sowohl die Fortran 77- als auch die Fortran 90- und die C-Bibliothek für den Einsatz auf zentralen Servern sowie auf Institutsrechnern zur Verfügung.

Neben der Weiterentwicklung dieser Bibliotheken hat die NAG Ltd. in den vergangenen Jahren zusätzliche parallelisierte Bibliotheken entwickelt, die sich durch eine hohe Effizienz auszeichnen. Durch den Einsatz dieser Bibliotheken kann ein erheblicher Aufwand bei der Programmentwicklung eingespart werden.

Die NAG-HPC Bibliotheken umfassen

- die NAG Parallel MPI Library für Parallelrechner

mit verteiltem Speicher (z. B. IBM-SP oder Linux Cluster) sowie

- die NAG SMP Library für Mehrprozessorsysteme mit gemeinsamem Speicher.

Beide Produkte werden in einer Informationsveranstaltung unter dem Titel "HPC Numerical Libraries: Current Successes and Future Challenges" von Dr. Stefano Salvini, NAG Ltd. UK, am 04.12.2002 vorgestellt.

Herr Salvini wird die Produktpalette der NAG Ltd., insbesondere die parallelisierten NAG HPC-Bibliotheken sowie Benchmarks für verschiedene Architekturen (z. B. IBM Power 4, etc.) erläutern.

Teilnehmer an dieser Informationsveranstaltung können auch gerne Code zur Analyse oder bestimmte Problembeispiele zur Diskussion mitbringen.

Datum: Mittwoch, 4. 12. 2002

Zeit: 10.00 bis 12.00 Uhr

Ort: RZ, Raum 217, 2. OG

Nikolaus Geers, Tel. -3755,

E-Mail: geers@rz.uni-karlsruhe.de.

Computer und Recht

Der Kopierschutz nach Änderung des Urheberrechts

Rechtsanwalt Dr. Stefan Ernst, Freiburg/Br.

Noch ist die letzte Reform nicht erkaltet und das neue Urhebervertragsrecht gerade erst wirksam, da steht bereits die nächste Neuerung an. Zum 01.01.2003 soll eine weitere Urheberrechtsnovelle in Kraft treten. Das im Entstehen befindliche Gesetz dient der Umsetzung der Richtlinie des Europäischen Parlaments und des Rates vom 22.05.2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft.

Es ist dies die jüngste von mittlerweile sieben EU-Richtlinien auf dem Gebiet des Urheberrechts. Gleichzeitig ist es eine von vielen Richtlinien, die sich mit den rechtlichen Aspekten der Informationsgesellschaft und damit auch des elektronischen Geschäftsverkehrs befassen. Nach dem ersten Referentenentwurf vom 18.03.2002 liegt inzwischen aus dem Bundesjustizministerium ein Regierungsentwurf mit dem Stand vom 31.07.2002 vor, der Gegenstand des folgenden Beitrags ist. Zu beachten bleibt allein, dass die vorliegende Gesetzesfassung im Gesetzgebungsverfahren noch verändert werden kann.

Vorbemerkung

1. Allgemeines

Das Urheberrecht ist – ungeachtet seiner ältesten Wurzeln – immer noch ein Kind der Technik. Erst die Erfindung des Buchdrucks ließ die Notwendigkeit eines Schutzes des Schöpfers kultureller Werke offenbar werden. Aus ihr ergab sich die Erforderlichkeit staatlicher Regulierung, deren Novellierungen ebenfalls fast stets mit technischen Entwicklungen einhergingen. Dabei waren die Gerichte naturgemäß dem Gesetzgeber ein wenig voraus. Dem europäischen Gesetzgeber obliegt freilich in erster Linie die Harmonisierung des nationalen Rechts, doch gibt auch die nunmehr umzusetzende Richtlinie ungeachtet dessen eine Vielzahl von technisch bedingten Normen vor, für die es bislang kein nationales Vorbild gibt.

2. Urheberinteressen und Kopierschutz

Angesichts der unbeschränkten Kopiermöglichkeiten in Originalqualität hat das Interesse der Industrie an „digitalem Selbstschutz“ erheblich zugenommen. Dieser kann im Wesentlichen nur aus Zugangskontrollen und Kopiersperren bestehen. Dass damit Kollisionen zu den Nutzerinteressen auftreten müssen, ist offenbar, denn der Kopierschutz wirkt nicht nur gegen illegale Piraterie, sondern auch gegen berechtigte Nutzung. Dies gilt auch und gerade für das Recht zur privaten Vervielfältigung. So sehr auch die Zulassung von Privatkopien – gegen Vergütung durch die Geräte- und Leerkassettenabgabe - für analoge Werke die einzig sinnvolle Lösung gewesen ist, so problematisch bleibt die Lage auf dem digitalen Markt. Durch das Internet sind Kopien in bisher nicht da gewesener Zahl möglich geworden, so dass die Rechteinhaber verständlicherweise zu Maßnahmen greifen, die von vornherein jede Vervielfältigung verhindern. Dass diese Kopierschutzsysteme dabei keinen Unterschied zwischen zulässiger und unzulässiger Nutzung machen können, liegt auf der Hand. Allein sie können verhindern, dass massenhaft neue Vervielfältigungsstücke in Originalqualität entstehen. So ist denn die Regelung des Schutzes solcher technischen Maßnahmen der bemerkenswerteste Part der vorgesehenen Novelle. Die in den einschlägigen Normen umgesetzten Vorschriften der Richtlinie beruhen dabei ihrerseits bereits auf (allgemein gehaltenen) Verpflichtungen aus den internationalen Abkommen.

3. Abgrenzung zu Zugangskontrolldiensten

Das Urheberrecht kann nur die Frage der Kopiersperren regeln. Der parallele Schutz durch Zugangskontrollen wird im ebenfalls recht jungen Zugangskontrolldiensteschutzgesetz behandelt. Zugangskontrolldienste sind technische Verfahren oder Vorrichtungen, die die erlaubte Nutzung eines zugangskontrollierten Dienstes ermöglichen. Solche Dienste können entgeltliche Rundfunk-, Tele- oder auch Mediendienste sein. Das Gesetz verbietet strafbewehrt die Herstellung, Einfuhr und Verbreitung von Umgehungsvorrichtungen zu gewerbsmäßigen Zwecken, bußgeldbe-

wehrt Besitz, Einrichtung, Wartung und Austausch dieser Vorrichtungen zu gewerbsmäßigen Zwecken und (unbewehrt) die Absatzförderung.

Hier geht es also um die Überwindung etwa von Pay-TV oder kostenpflichtigen Online-Zugängen im Wege des Hacking, was für den Täter selbst schon im Strafgesetzbuch unter Strafe steht. Das neue Gesetz weitet die Verantwortlichkeit auf die Verbreiter der entsprechenden Vorrichtungen aus.

Schutz technischer Maßnahmen

Im Folgenden wird die im Regierungsentwurf beschriebene neue Rechtslage im Einzelnen vorgestellt. Der Gesetzestext selbst ist recht unübersichtlich und sprachlich für den Laien kaum zugänglich, da den Entwurfsverfassern die möglichst wörtliche Umsetzung der Richtlinie geboten schien.

1. Schutz technischer Maßnahmen

a) Definition

Der Gesetzentwurf definiert den Schutzgegenstand der Norm – wirksame (nicht: unumgehbare) technische Maßnahmen – als Technologien, Vorrichtungen und Bestandteile, die im normalen Betrieb dazu bestimmt sind, bestimmte Verwertungshandlungen – insbesondere das Kopieren - durch das Urheberrechtsgesetz geschützter Werke oder Schutzgegenstände zu verhindern. Gemeint sind insbesondere Zugangskontrollen, Verschlüsselung und Kopierschutzvorrichtungen. Technische Schutzmaßnahmen werden unabhängig von der verwendeten Technologie vor Umgehung geschützt. Die Norm gilt also sowohl für Hardware- (z. B. Dongles) als auch für Software-Schutzmaßnahmen.

b) Umgehungsverbot

Technische Schutzmaßnahmen der genannten Art dürfen ohne Zustimmung des Rechteinhabers nicht umgangen werden, um Zugang zum geschützten Werk zu erhalten. Das Kopieren eines urheberrechtlich geschützten Werkes oder eines anderen durch das Urheberrechtsgesetz geschützten Schutzgegenstandes unter Umgehung eines Kopierschutzes ist demnach verboten. Dies gilt ungeachtet der urheberrechtlichen Schrankenbestimmungen, die in bestimmten Fällen auch ungefragtes Kopieren – zum Teil gegen Entgelt – gestatten. Zur Durchsetzung dieser Schrankenbestimmungen hat der Gesetzgeber eine eigene Norm vorgesehen, die unten vorgestellt (2.) wird. Allein Umge-

hungshandlungen zu wissenschaftlichen Zwecken (z. B. Kryptografie) werden nicht erfasst.

c) Vertrieb von Hacking-Werkzeugen

Der nächste Absatz regelt das Verbot von Hacking-Werkzeugen, greift also bereits im Vorfeld der oben genannten Handlungen ein. Gemeint sind Vorrichtungen, Erzeugnisse oder Bestandteile, die die Umgehung technischer Schutzmaßnahmen beabsichtigen (Nr. 1), solche Vorrichtungen, die von der Umgehung abgesehen nur einen begrenzten wirtschaftlichen Nutzen haben (Nr. 2) oder hauptsächlich dazu dienen, diese Umgehung zu ermöglichen oder zu erleichtern (Nr. 3).

Dabei ist zu erwarten, dass es hinsichtlich der Varianten 2 sowie 3 und der Abgrenzung zu erlaubten Geräten und Software, die das Kopieren ebenfalls erleichtern können, in der Zukunft vielfältigen Streit geben wird.

Verboten sind die Herstellung, Einfuhr, Verbreitung (insbesondere Verkauf und Vermietung, aber auch Verleih und kostenlose Weitergabe) sowie die Werbung für diese Werkzeuge. Ausdrücklich verboten ist aber auch schon der - zu gewerblichen Zwecken dienende - Besitz von Hacking-Werkzeugen oder die Erbringung entsprechender Dienstleistungen.

d) Strafverfolgung und polizeiliche Gefahrenabwehr

Allein Polizei und Strafverfolgungsbehörden dürfen die beschriebenen Verbote in Erfüllung ihrer Pflichten ausdrücklich umgehen.

2. Durchsetzung von Schrankenbestimmungen

In den Normen des Gesetzes sind diverse Schranken des Urheberrechts normiert. Diese dienen dazu, im Interesse der Kulturwirtschaft und der Allgemeinheit u. a. die Nutzung und auch das Kopieren urheberrechtlich geschützter Werke zwar zum Teil gegen Entgelt, aber in jedem Fall auch gegen den Willen des Rechteinhabers zu gestatten - damit diese Schranken durch den Einsatz von Kopiersperren nicht leer laufen, wurden Verpflichtungen zu Lasten des Rechteinhabers formuliert. Soweit diese technischen Maßnahmen eine ansonsten berechnete Nutzung verhindern, ist den Begünstigten bestimmter Schranken die Umgehung des entsprechenden Schutzes zu ermöglichen. Es handelt sich dabei um die Schranken zu Rechtspflege und öffentlicher Sicherheit, für Behinderte, Schul- und Unterrichtsgebrauch, Schulfunksendungen, öffentliche Zugänglichmachung für Unterricht und Forschung, Archiv, eigene Unterrichtung und sonstiger eigener

Gebrauch, jeweils in Papierform oder nichtwirtschaftlich und für Sendeunternehmen. Das Recht zur privaten Vervielfältigung ist nur betroffen, soweit es um die Vervielfältigung in Papierform oder ähnliche Träger geht, nicht aber auf Bild-, Ton- oder Datenträger.

Wie die Berechtigten ihrer Verpflichtung nachkommen, ist diesen freigestellt. So mögen etwa Schlüsselinformationen an die durch die Schranken privilegierten Personen und Institutionen weitergegeben werden. Dies kann aber auch auf Verbände beschränkt werden, wenn die Erfüllung der Pflichten damit gesichert ist. Nicht zuletzt mag auch die Möglichkeit zum Online-Abruf weiterer Vervielfältigungsstücke hinreichend sein.

Dies bedeutet aber nicht, dass in diesen Fällen der Einsatz von Kopierschutzknackern gestattet würde. Der Entwurf gewährt dem Berechtigten der genannten Schrankennormen lediglich einen Anspruch gegen den Hersteller darauf, ihm die zur Wahrnehmung der Rechte benötigten Mittel zur Verfügung zu stellen. Es gibt keine Möglichkeit zur Selbsthilfe, kein „right to hack“. Dass diese Regelung freilich die Anspruchsdurchsetzung verzögern und zuweilen ganz verhindern kann (insbesondere bei Fällen mit Auslandsbezug) ist eine andere Frage. Neben dem allgemeinen Prozessrisiko ist dies stets zumindest mit zeitlichem Aufwand und Verzögerung verbunden. Aus diesem Grunde wird mit der Rechtsänderung zugleich eine Ergänzung des Unterlassungsklagengesetzes eingeführt, das eine Prozessführung etwa durch Verbraucherverbände und Kammern ermöglicht.

3. Schutz der zur Rechtswahrnehmung erforderlichen Informationen

Der Entwurf verbietet grundsätzlich die Veränderung von werkintegrierten Informationen, die der Berechtigte zur Erleichterung der Rechtswahrnehmung angebracht hat. Das Gesetz definiert dies als elektronische Informationen, die das Werk selbst oder den Rechteinhaber identifizieren oder auch Informationen über Nutzungsmodalitäten enthalten.

Hierunter fallen also zum einen spezielle dem Schutz dienende Instrumente wie zum Beispiel digitale Wasserzeichen. Unter die Norm fällt aber auch die Veränderung von einfachen Informationen etwa die automatische Nennung des Autors einer Textdatei unter „Eigenschaften“. Wurde die Information verändert oder entfernt, darf das Werk nicht mehr weitergegeben oder öffentlich wiedergegeben werden.

4. Kennzeichnungspflichten

Damit der Käufer über technische Schutzmaßnahmen bei einem Werk sofort informiert ist, ist geboten, dass auf diese deutlich sichtbar und mit Angaben zu den Eigenschaften des Schutzes hingewiesen wird. Das Kennzeichnungsgebot dient also dem Verbraucherschutz. Fehlt ein solcher Hinweis und ist das erworbene Werkstück aus diesem Grunde für den Käufer nicht nutzbar, kann er Gewährleistungsrechte (Neulieferung, gegebenenfalls Umtausch) geltend machen.

5. Keine Geltung für Software

Die Normen zum technischen Schutz sollen auf Computerprogramme keine Anwendung finden. Dies ist dadurch bedingt, dass die hier umgesetzte Richtlinie auf Computerprogramme keine Anwendung findet und Abgrenzungsprobleme zum Recht zur Erstellung einer Sicherungskopie und zu den Regelungen zur Dekompilierung vermieden werden sollen. Die meisten Schranken, insbesondere eine freie Kopie zum Privatgebrauch, sind bei Software ohnehin vom Gesetz nicht vorgesehen.

Straf- und Bußgeldnormen

1. Strafbarkeit unerlaubter Eingriffe

Ein zahnlöser Tiger verbreitet relativ wenig Schrecken. Der vorgesehene Schutz wird aus diesem Grunde mit kräftigen Mitteln untermauert. Dies entspricht der erforderlichen Umsetzung der Richtlinie, die angemessene Sanktionen für alle Pflichten verlangt. Wer gegen die oben beschriebenen Verbote verstößt, kann sich strafbar machen, auch wenn eine Strafverfolgung nur bei Vorliegen eines Strafantrags erfolgt. Das Strafmaß wird bei gewerbsmäßigem Handeln erhöht. Strafbar sind demnach im Einzelnen:

- die Umgehung eines Kopierschutzes in der Absicht, sich oder einem anderen Zugang zu einem geschützten Werk zu verschaffen;
- die Entfernung einer Information für die Rechtswahrnehmung, also z. B. eines digitalen Wasserzeichens;
- die Einfuhr, Verwertung oder öffentliche Wiedergabe eines Schutzgegenstandes, bei dem etwa z. B. ein Wasserzeichen entfernt wurde;
- die Herstellung, Einfuhr, Verbreitung, Verkauf, Vermietung eines Kopierschutzknackers zu gewerblichen Zwecken.

2. Strafflosigkeit bei privatem Gebrauch

Strafflos bleibt allerdings die Tat, die ausschließlich zum eigenen privaten Gebrauch des Täters oder mit dem Täter verbundener Personen erfolgt oder sich auf einen derartigen Gebrauch bezieht. Die persönliche Verbindung im Sinne der Norm ist aber eng allein im Sinne des Familien- und Freundeskreises auszulegen.

3. Ordnungswidrigkeiten

Aufgrund des geringeren Unrechtsgehalts lediglich ordnungswidrig, aber immer noch bußgeldbewehrt handelt, wer

- Kopierschutzknacker nicht gewerbsmäßig verkauft,

vermietet oder an Personen weitergibt, die nicht mit ihm persönlich verbunden sind;

- Kopierschutzknacker zu gewerblichen Zwecken besitzt;
- für den Verkauf oder die Vermietung von Kopierschutzknackern wirbt;
- entsprechende Dienstleistungen erbringt.

Auf der anderen Seite wird aber auch der Rechteinhaber mit Bußgeld bedroht, wenn er die geforderten Mittel zur Nutzung der Urheberrechtsschranken nicht zur Verfügung stellt oder seinen Kennzeichnungspflichten nicht oder nicht vollständig nachkommt.

Personalia



Foto: sl

Frau **Petra Haberer** ist seit dem 3. Juni 2002 in der Abteilung Anwendungs- und Softwaresysteme für das Teilprojekt Campus Mobile Communication Center

(CMCC) im Projekt Notebook-University (NU-KATH) eingestellt.

Mit dem Projekt Notebook-University soll die alltägliche Ausbildung an der Universität Karlsruhe um mobilitätsunterstützende Dienste und E-Learning-Umgebungen für verschiedene Fakultäten bereichert werden. Ziel des Teilprojekts CMCC ist dabei die Entwicklung von allgemeinen und anwendungsspezifischen Basisdiensten in interdisziplinärer Zusammenarbeit mit anderen Teilprojekten. Dazu muss eine nahtlose globale Infrastruktur für verschiedene Wireless-Technologien (WLAN, GPRS, UMTS) entwickelt werden. CMCC wird gemeinsam vom Rechenzentrum und dem BMBF getragen.

Der Arbeitsplatz von Frau Haberer befindet sich im Raum 052, Tel. -8104, E-Mail: petra.haberer@rz.uni-karlsruhe.de

Vorträge, Workshops und Kurse *auf einen Blick*

Leiterplatten-Entflechtung:

Vorstellung des Programms Expedition PCB

Dieter Kruk

Datum: 28.11.2002
Zeit: 16.15 - 17.00 Uhr
Ort: RZ, Raum 217, 2. OG

Arbeitskreis Linux Cluster an der Universität Karlsruhe

Nikolaus Geers

Datum: 13.11.2002
Zeit: 14.00 - 16.00 Uhr
Ort: RZ, Raum 217, 2.OG

Präsentation der NAG HPC-Libraries

Nikolaus Geers

Datum: 4.12.2002
Zeit: 10.00 - 12.00 Uhr
Ort: RZ, Raum 217, 2.OG

Neues Werkzeug für Finite Elemente

Die CAE-Umgebung Altair Hyper Works 5.1

*Altair Engineering GmbH
Dr. Paul Weber, RZ*

Datum: 8. 11. 2002
Zeit: 9.00 - ca. 12.00 Uhr
Ort: RZ, Raum 217, 2. OG

Die folgenden Kurse werden von Frau Margret Schneider durchgeführt und finden jeweils in der Zeit von 18.00 Uhr bis 19.30 Uhr statt.

Einführungskurs Internet II

Datum: 31.10.2002
Ort: RZ, Raum 217, 2. OG

Einführungskurs UNIX/Linux-Grundlagen

Datum: 07.11.2002
Ort: RZ, Raum 217, 2. OG

Einführungskurs Web/HTML

Datum: 14.11.2002
Ort: RZ, Poolraum A, UG

Einführungskurs Sicherheit im Internet

Datum: 21.11.2002
Ort: RZ, Raum 217, 2. OG

Netzwerktechnik I & II

Datum: 28.11. und 05.12.2002
Ort: RZ, Raum 217, 2. OG

Linux: Einstieg, Distributionen und erste Schritte

Datum: 12.12.2002
Ort: RZ, Raum 217, 2. OG

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

BIT8000 (Help Desk)	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
MicroBIT-Hotline	Tel. -2997, E-Mail: microbit@rz.uni-karlsruhe.de
Scientific Supercomputing Center (SSC) Karlsruhe	Tel. -8011, E-Mail: contact@ssc.uni-karlsruhe.de
Anwendungen	Tel. -4031/4035, E-Mail: anwendung@rz.uni-karlsruhe.de
Netze	Tel. -2068/4030, E-Mail: netze@rz.uni-karlsruhe.de
UNIX	Tel. -4038/4039, E-Mail: unix@rz.uni-karlsruhe.de
Virus-Zentrum	Tel. 0721/9620122, E-Mail: virus@rz.uni-karlsruhe.de
Mailing-Liste 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
Multimedia Transfer	Tel. -4873/-6113, E-Mail: kontakt@mmt.uni-karlsruhe.de

Öffentliche Rechnerzugänge

World Wide Web:

<http://www.rz.uni-karlsruhe.de/> (Informationssystem des Rechenzentrums der Universität Karlsruhe)
<http://www.uni-karlsruhe.de/Uni/CA/> (Zertifizierungsstelle am Rechenzentrum der Universität Karlsruhe)

Ftp:

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