

## **Arbeitsbereich Anwendungen der Informatik in Geistes- und Naturwissenschaften (AGN)**

Vogt-Kölln-Str. 30, Haus C, D-22527 Hamburg,

Tel.: +49 40 428 38- 2406, Fax: 040 / 428 83- 2226

URL: <http://agn-www.informatik.uni-hamburg.de>

### **1. Zusammenfassende Darstellung**

#### **Mitglieder des Arbeitsbereiches**

##### *Professoren:*

Dipl.-Phys. Dr. rer. nat. Klaus Brunnstein (Leiter des Arbeitsbereiches)

##### *Assistentinnen/Wiss. Mitarbeiterinnen:*

Dipl.-Inform. Arslan Brömme

Dipl.Inform. Marian Kassovic (bis 30.4.2001)

N.N. (ab 1.5.2001)

##### *Technisches und Verwaltungspersonal:*

Margit Leuschner

### **Allgemeiner Überblick**

Der Arbeitsbereich hat sich seit seiner Gründung (1972 als eine der ersten Forschungsgruppen des damals neu gegründeten Instituts für Informatik) zunächst auf Informatik-Aspekte des Computer-Gestützten Unterrichts (FG CGU) konzentriert. In diesem Rahmen sind erste Schulversuche zu Informatikthemen (im Rahmen des Mathematik-Unterrichts) an mehr als 10 Hamburger Gymnasien und Gesamtschulen durchgeführt worden, wobei jeder Schule eine Minirechner (Digital Equipment PDP-8) mit schulspezifischer Software zur Verfügung gestellt wurde; diese Projekte wurden im Rahmen des damaligen Forschungsprogrammes „DV im Bildungswesen“ des Bundes-Forschungsministeriums (dessen Leitungsgremium der Leiter der Forschungsgruppe angehörte) den Schulen unentgeltlich zur Verfügung gestellt. Ergänzend wurden rund 20 Lehrer – in Zusammenarbeit mit dem Institut für Lehrbildung – in Themen der Informatik eingeführt. Die Kultusbehörden in Hamburg, Niedersachsen und Rheinland-Pfalz wurden auch bei der Entwicklung der ersten (freiwilligen) Curricula für Schul-Informatik unterstützt.

Ein weiterer Schwerpunkt lag auch in der Untersuchung, wie innovative Informatikmethoden in Geistes- und Naturwissenschaften sowie in der Medizin eingesetzt werden können. Das Arbeitsgebiet Medizin – in dem an der Universität seit 1974 das erste Curriculums für das Nebenfach (heute: Ergänzungsfach) Medizin für Informatik-Studierende angeboten

wurde – wurde vom Leiter der Forschungsgruppe aus seinem Auftrag bei seiner vorherigen Institution (Deutsches Elektronen-Synchrotron DESY) entwickelt, die Universitätskliniken Eppendorf (UKE) über das DESY-Rechenzentrum mit Computermethoden zu unterstützen (der FG-Leiter hat 1970-1972 ein erstes Computerverfahren anstelle der manuellen Analyse im Labor der 2. medizinischen Klinik programmiert und eingeführt; dieses Projekt DESY-UKE wurde anschließend von Dr. Höhne fortgeführt). Bei den geisteswissenschaftlichen Anwendungen stand die Analyse und Kritik der vorherrschenden Paradigmen in der Informatik sowie einer Einschätzung der Wirkungen von Informations- und Kommunikationstechniken; diese Themen werden auch heute noch bearbeitet.

Seit Mitte der 80'er Jahre haben sich die Aktivitäten des Arbeitsbereiches vor allem auf Datenschutz, verschiedene rechtliche Aspekte der Informatik (vom Schutz intellektuellen Eigentums bis zur Forensischen Informatik) sowie auf die technische Sicherheit und die Aufklärung von Unfällen Computer-Gestützter Systeme und von Netzunfällen konzentriert. Die Schwerpunkte der Forschung orientieren sich an dem Ziel, Sicherheitsmängel heutiger Systeme zu erkennen und solche Mängel soweit möglich durch systemische oder andere Maßnahmen einzuschränken oder auszugleichen.

1988 wurde das „Virus Test Center“ (VTC) gegründet – bis heute weltweit das einzige Universitätslabor dieser Art, welches seit 1990 das Bundesamt für Sicherheit in der Informationstechnik (BSI) als Notfallteam beim Auftreten bössartiger Software unterstützt; in diesem Gebiet sind zahlreiche praktische Hilfestellungen für Firmen, Institute und Personen bei Virenvorfällen erfolgt. Seit 1994 werden im Network Test Center (NTC) zunächst Sicherheitsaspekte lokaler Netze (LANs), seit 1996 zunehmend auch Sicherheitsdefizite des InterNetworking untersucht. Auch wurde der Aufbau des Computer-Notfallteams (Computer Emergency Response Team) des Deutschen Forschungsnetz am Rechenzentrum des FB Informatik (Leiter: Dr. Mück) wissenschaftlich begleitet (u.a. wurden 3 Doktorarbeiten betreut).

Im AB AGN wurde seit 1988/89 - erstmalig in Europa - ein 4-semestriges Veranstaltungsangebot „Einführung in die IT- und Netz-Sicherheit“ im Rahmen des Vertiefungsgebietes „IT-Sicherheit/Datenschutz (ITDS)“ angeboten. Diesen Zyklus (von WS 1988/89 bis SS 2001, also in 7 Zyklen) haben mehr als 400 Studierende gewählt, und es sind rund 100 Examensarbeiten – Studien/Diplomarbeiten - und Doktorarbeiten aus diesen Themengebieten erstellt worden (siehe auch die Internet-Seite des AB AGN). Seit Sommersemester 2001 wird die neue Vorlesung „Grundlagen Beherrschbarer Informatiksysteme“ (GBI) im Rahmen des „neuen“ Bachelor/Diplomstudienganges für Studierende der Informatik sowie der Wirtschaftsinformatik angeboten, in welcher (in 4 SWS, also knapp 60 Wochenstunden) ein Überblick über Sicherheitsprobleme, wirtschaftliche und rechtliche Rahmenbedingungen sowie über Lösungsansätze und Praxis der IT-Sicherheit angeboten wird.

**Forschungsschwerpunkte des Arbeitsbereiches:**

- IT- und Netz-Sicherheit sowie Datenschutz
- Risikoanalyse und Unfallanalyse von Computer- und Netzsystemen
- Forensische Informatik
- Rechtliche und gesellschaftliche Aspekte der Informationsgesellschaft
- Ethische Aspekte der IuK-Technologien

**Wissenschaftliche Zusammenarbeit**

- Koordination und Zusammenarbeit mit AntiViren-Fachleuten (CARO= Computer antivirus Research Organisation, ein Zusammenschluss wichtiger Fachleute zur Zusammenarbeit bei der Aufklärung neuartiger Bedrohungen)
- Zusammenarbeit mit zahlreichen Universitäten in Europa und USA über „Safety Critical Systems“ (u.a. im Bereich der Sicherheit von Avionik-Systemen und der Untersuchung von Flugunfällen auf eventuelle Technik-bedingte Ursachen)
- Zusammenarbeit mit Universität Stockholm, Lund Universität, Copenhagen Business School, TU Graz, Universität Wien, Gesamthochschule Essen, Universität Oulu, Aristoteles Universität Thessaloniki, Athens University of Economics & Business, Universität Patras, Universität Piräus, Ägäische Universität, Universitäts College Dublin, Universität Aston, Universität Kingston, Universität London (Royal Holloway), Universität Plymouth, Katholische Universität Leuven, Universität Rom-La Sapienza im Rahmen der Erasmus/Sokrates-Projekte- 29770-IC-1-96-1-DE-ERASMUS-EPS-1, 29118-IC-1-96-GR-ERASMUS-EPS-1.

**Ausstattung**

Die Rechner-Ausstattung des Arbeitsbereiches AGN wird im folgenden nach Projekten beschrieben. Im Projekt **Virentests** befinden sich insgesamt 7 Pentium Rechner (90, 133, 200, 233), zwei Pentium II (233), sowie fünfzehn 486/50; ein Teil dieser Geräte wurde von Unternehmen gespendet. Zusätzlich werden zum Dauertest ein 286/10 und ein 386/20 eingesetzt. Der **WWW-Server** läuft auf einem Pentium II 333. Im **Arbeitsbereichsnetz**, das für allgemeine Arbeiten der Studien- und Diplomarbeiten, sowie für Projektarbeiten zum Thema **Netzwerktests** im Bereich Win95, NT, OS/2 und Novell sowie **Chipkarten** und **Untersuchungen biometrischer Verfahren** vorgesehen ist, befinden sich sechs Pentium II 350, vier Pentium II 233, ein Pentium 166, ein 486/50, ein 386/40, sowie ein Amiga 4000. Die **Mailbox** läuft auf einem 386/40. Die **Mitarbeiter** sind ausgestattet mit einem Pentium 133, zwei Pentium 166, einem Pentium 200 und einem Pentium II 350.

**Finanzmittel**

Spenden: dem Arbeitsbereich werden neben Geldspenden zur Beschaffung spezieller Geräte für IT-Sicherheitsuntersuchungen auch Geräte für die AntiViren-Tests zur Verfügung gestellt.

Drittmittel: siehe Erasmus/Socrates-Projekt  
Sonst: keine (siehe Anmerkung)

Anmerkung: Dem AB-Leiter ist die Beschränktheit der universitäten Mittel durchaus bewusst. Dennoch verfolgt er eine DMP-basierte Zusammenarbeit in seinem Fachgebiet aus grundsätzlichen Erwägungen nicht, zumal auch wegen eigener Erfahrungen mit früheren Projekten, wo wonach die Kreativität der Projektleiter unter bürokratischen Auflagen (Beantragung, Berichts- und Reisewesen) erheblich leidet. Im

Fachgebiet IT-Sicherheit/Unfallaufklärung ist der Aspekt der Unabhängigkeit der Fachleute sehr hoch zu bewerten; diese könnte durch die Teilnahme an Projekten gefährdet sein (z.B. hinsichtlich der Kritik an Schwerpunktsetzungen staatlicher Forschungsförderung etwa am Beispiel der Biometrik, in welcher der AB kompetent und engagiert ist). Im übrigen steht die Nicht-Teilnahme an Drittmittelforschung keineswegs im Widerspruch zu einem intensiven Erfahrungsaustausch mit im Bereich IT/Netz-Sicherheit tätigen Firmen, wie vom AB AGN häufig praktiziert.

In der täglichen Praxis erfolgt eine Beratung von Firmen und einzelnen Personen in zahlreichen Fällen beim vermuteten oder tatsächlichen Auftreten von Problemen, etwa von maliziöser Software. Auch werden regelmäßig Prüfungen der Erkennungsqualität von AntiMalware-Produkten von nahezu allen relevanten Herstellern durchgeführt und im Internet (oft nachgedruckt in einschlägigen Zeitschriften) publiziert. Diese insgesamt starke Unterstützung wirtschaftlicher Anwendungen erfordert ein hohes Maß an Unabhängigkeit und Glaubwürdigkeit, welche mit einer DMP-finanzierten Zusammenarbeit in wesentlichen Bereichen in Konflikt treten kann. Als etwa ein Staatsanwalt eine unabhängige Prüfung von Fehlern eines digitalen Telefonsystems anforderte, wurde dem AB-Leiter eröffnet, er müsse dieses Gutachten (obwohl nicht vereidigter Sachverständiger und anderweitig ausgelastet) anfertigen, weil alle einschlägig kompetenten Fachleute durch DMP-Mittel an den Anlagenbetreiber gebunden seien (dieser Betreiber hatte zuvor vergeblich versucht, auch mit dem AB eine DMP-Kooperation einzuleiten). Im übrigen unterstützen einige Unternehmen die Arbeit des Virus Test Center durch Spenden.

- Erasmus/Sokrates-Projekt- 29770-IC-1-96-1-DE-ERASMUS-EPS-1:  
Reisemittel für Studentenaustausch: 2800ECU  
Reisemittel für Dozentenaustausch: -- DM  
Reisemittel für Projekt: --DM
- Erasmus/Sokrates-Projekt- 29118-IC-1-96-GR-ERASMUS-EPS-1: 3000 ECU
- Projekt „Referenzstelle für Basisdokumentation“ mit BADO e.V.: 1200 DM

## 2. Die Forschungsvorhaben des Arbeitsbereichs

### 2.1 Risikoanalyse Computer-Gestützter Systeme

Brunnstein, K., Prof. Dr.

*Laufzeit des Projektes:*

1988-(2002)

*Projektbeschreibung:*

„Bösartige Software“ nimmt hinsichtlich Arten, Wirkung sowie Häufigkeit des Auftretens vor allem durch die zunehmende Vernetzung weiter erheblich zu. Neben Computer-Viren und Trojanischen Pferden erweitern vor allem Netz-Malware wie „böartige Applets“, maliziöse „ActiveX Controls“, Würmer und Agenten die Palette der Bedrohungen von Computer- und Netzsystemen.

Dieses Projekt hat die Aufgabe, bekannte sowie neuartige Bedrohungsformen zu analysieren und Methoden sowie Produkte geeigneter Gegenmaßnahmen auf ihre Wirksamkeit zu prüfen. Dazu werden umfangreiche Datenbanken entdeckter Malware vorgehalten; neben den umfangreichsten nicht-herstellergebundenen Datenbanken für PC-File- und PC-Boot-Viren dient die Makroviren-Datenbank als Referenz-Datenbank für die Benennung dieser Virenart nach CARO-Namenskonvention; die weltweite Kooperation von AntiViren-Fachleuten – CARO = Computer AntiVirus Research Organisation - wird vom AB-Leiter koordiniert. Auf Grundlage dieser Malware-Datenbanken werden zweimal jährlich Produk-

te wie AntiVirus-Software im Virus Test Center auf Erkennungsraten und Erkennungsqualität getestet; in diese Tests sind im Berichtsjahr jeweils 750 und 900 Stunden Arbeitszeit über einen Zeitraum von 4 bzw. 5 Monaten investiert worden. Die Testberichte werden im Frühjahr und Herbst auf den Internetseiten des AB veröffentlicht. Weiterhin wurde im Rahmen einer Diplomarbeit ein Verfahren erarbeitet, mit welchem die Reinigungsqualität von AntiVirus-Produkten bestimmt werden kann (Antivirus Repair Test, ART; erste Publikation im Herbst 2000).

Im Netz Test Center (NTC) werden vernetzte Betriebssysteme (Client+Server-Windows NT sowie Novell Netware 4) auf Schwächen und Angriffspunkte untersucht, und es werden Gegenmaßnahmen – insbesondere Firewalls sowie Einbruchs-entdeckende Experten Systeme - geprüft. Gemeinsam mit dem DFN-CERT (im FBI-RZ) werden Risiken heutiger Internet-Technologien untersucht und Verfahren zur Erhöhung der Sicherheit etwa mit verbesserter Authentizität (Doktorarbeit S. Kelm), Methoden der Behandlung von Computer/Netzunfällen (Doktorarbeit K-P. Kossakowski) sowie sichere Breitbandkommunikation (Mitbetreuung der Doktorarbeit von C. Benecke) behandelt. Das umfangreiche Wissen über böartige Software und Unsicherheiten von Computer- und Netzsystemen wird bei regelmäßiger Nachfrage auch betroffenen Unternehmen und Personen zur Erkennung und Behebung von unerwünschten Vorfällen zur Verfügung gestellt.

*Schlagwörter:*

Computer-Viren, Computer-Würmer, Trojanische Pferde, Malware, Hacking, Angriffe, Computer Incidents, Forensische Informatik

*Publikationen aus dem Projekt:* (siehe Publikationsliste)

## **2.2 Unfallanalyse von Computer- und Netzsystemen bei kritischen Anwendungen**

Brunnstein, K., Prof. Dr.

*Laufzeit des Projektes:*

1990-(2002)

*Projektbeschreibung:*

In Erweiterung des klassischen Computer-Sicherheitsbegriffes („security“) wird untersucht, welche weitergefaßten (=holistischen) Sicherheitsaspekte („safety“) beim Einsatz von Realzeitsystemen und in neuartigen, u.U. kritischen wirtschaftlichen Anwendungen wie „Electronic Banking“ oder „Electronic Commerce“ zu fordern sind. Dabei sind zur Beherrschbarkeit etwa von Verkehrskontrollsystemen (z.B. Digitale Avionik) neben Verlässlichkeit und Verfügbarkeit vor allem Aspekte wie Funktionalität oder zeitliche Korrektheit zu gewährleisten.

Netzangriffe auf Unternehmen sind oft auf unzureichende Stabilität, Konsistenz und Persistenz von Systemen, Programmen und Daten zurückzuführen. In diesem Fachgebiet werden neben grundsätzlichen Arbeiten über die Bestimmung des „holistischen Sicherheitskonzeptes“ auch aktuelle Unfälle (z.B. Internet-gestützter Handlungen und Methoden) analysiert, und ihre paradigmatischen Ursachen werden untersucht. In früheren Phasen

wurde u.a. ein „Flight Incident Analysis Tool“ nach einer Spezifikation der Flug-Unfall-Untersuchungsstelle des Luftfahrtbundesamtes in einer Diplomarbeit ausgearbeitet und vorgestellt. Aktuell werden jeweils bei gegebenem Anlass gezielte Analysen des „Computer-Anteiles“ aktueller Flugzeugunglücke – hier in enger Zusammenarbeit mit einem Kreis einschlägig interessierter Informatiker und Avioniker, koordiniert über das Internet – wird eine Dokumentation für Computer/Netz-Unfälle aufgebaut (Verwendung für Vorträge, Vorlesungen sowie für ein geplantes Buch über „Paradigmen der Informatik und ihre Wirkungen“).

*Schlagwörter:*

Computer Incidents, Forensische Informatik, Beherrschbarkeit der Informationstechnik

*Publikationen aus dem Projekt:* (siehe Publikationsliste)

### **2.3 Datenschutzgerechte Gestaltung von Sicherheitsmechanismen**

Nachdem Frau Dr. Fischer-Hübner einen Ruf auf eine Informatik-Professur an der Universität Karlstadt/Schweden (2000) angenommen hat, wird dieses Projekt im Rahmen von studentischen Examens- sowie Doktorarbeiten vom AB-Leiter fortgeführt.

Gegründet von: Fischer-Hübner, Simone, Dr.

*Laufzeit des Projektes:*

10/ 92 - 12/ 2000

*Projektbeschreibung:*

Auf dem Weg in die Globale Informationsgesellschaft mit einer steigenden Gefährdung des Datenschutzes, gewinnen Datenschutztechnologien zunehmend an Relevanz. In diesem Projekt werden Kriterien, Modelle und Konzepte für datenschutzgerechte Systeme erarbeitet.

Die heutigen Sicherheitsmodelle und -systeme sind in der Regel kaum geeignet, juristische Datenschutzerfordernungen (etwa Zweckbindung, Verhältnismäßigkeit) hinreichend zu gewährleisten. Es ist daher ein formales aufgabenbasiertes Datenschutzmodell zur technischen Durchsetzung gesetzlicher Datenschutzerfordernungen entworfen worden. Es wurde spezifiziert, wie dieses Datenschutzmodell nach dem "Generalized Framework for Access Control" (GFAC)-Ansatz in Unix System V umgesetzt werden kann. In dem Projekt "Rule Set-based Access Control" (RSBAC), welche ursprünglich als Diplomarbeitprojekt anging, wurde dieses Datenschutzmodell nach dem GFAC-Ansatz zusammen mit anderen Sicherheitsmodellen in Linux implementiert. Weiterhin wurde die Entscheidungskomponente des resultierenden RSBAC-Systems um heuristische Sicherheitsregeln ergänzt. Es ist angedacht mit Hilfe von Autorisierungszertifikaten (genauer: SPKI-Zertifikaten) das RSBAC-System für eine verteilte Zugriffskontrolle auszubauen, welche auch die Zugriffsberechtigungsprüfung von anonym agierenden Benutzern gestattet.

Weiterhin wurden gemäß dem Prinzip der Vermeidung personenbezogener Daten Konzepte zur Pseudonymisierung von benutzerbezogenen Kontrolldaten analysiert, vorgeschlagen, angewendet, durch welche Sicherheitsmechanismen datenschutzkonform gestaltet werden sollen. So können insbesondere durch eine Pseudonymisierung von benutzerbezogenen Audit- oder Profildaten (pseudonymes Auditing) Auditing und Intrusion Detection Systeme

datenschutzgerecht gestaltet und somit dem Konflikt zwischen Datenschutz und IT-Sicherheit begegnet werden.

*Schlagwörter:*

Datenschutzkonforme Systeme (Privacy-Enhancing Technologies), Pseudonymität, pseudonymes Auditing, aufgaben-basiertes Datenschutzmodell, Sicherheitsmodelle, GFAC, RSBAC

*Publikationen aus dem Projekt: (siehe Publikationsliste)*

## **2.4 Vertrauenswürdige Kommunikation im elektronischen Zahlungsverkehr - ein Rollen- und Aufgabenbasiertes Sicherheitsmodell für Anwendungen mit multifunktionalen Chipkarten**

Nachdem Frau Dr. Schier die Universität Hamburg zwecks praktischer Tätigkeit bei einem Finanzinstitut verlassen hat, wird dieses Projekt im Rahmen von studentischen Examensarbeiten fortgeführt.

Gegründet von: Schier, K., Dipl.-Inform.

*Laufzeit des Projektes:*

09/94 - 07/99

*Projektbeschreibung:*

Chipkarten finden immer weitere Verbreitung in allen Bereichen des täglichen Lebens (Gesundheitswesen, Bank- und Finanzwesen, usw.). Die Chipkarte ist nur ein Element, das zu einer sicheren Übertragung führen kann. Sicherheitsbetrachtungen bei Chipkarten-Anwendungen führen automatisch zu Problemen der sicheren Übertragung in verteilten Systemen. Weitergehend müssen prinzipielle Probleme bei der Übertragung sensibler Informationen über unsichere Kanäle betrachtet und gelöst werden. Welche Sicherheitskonzepte kann man in welchen Anwendungssituationen realisieren?

Als spezielle Anwendungssituation wird der elektronische Zahlungsverkehr untersucht. Welche Protokolle existieren zur Zeit, um elektronische Zahlungsvorgänge zu ermöglichen. Welchen Sicherheitsanforderungen genügen diese Konzepte und welche Anforderungen werden nicht erfüllt? Ziel ist es, ein generisches Sicherheitskonzept zu entwickeln, das unter Betrachtung des jeweiligen Restrisikos eine umsetzbare Sicherheitspolitik zulässt. Es wird ein Sicherheitsmodell entwickelt, das eine Kombination des rollenbasierten und aufgabenbasierten Zugriffsmodells darstellt. Durch die individuelle Gestaltung des Rollen- und Aufgabenkontextes kann ein individuelles Sicherheitsumfeld für jeden Benutzer geschaffen werden. Die Implementierung des Modells erfolgt im Betriebssystem einer Chipkarte.

*Schlagwörter:*

Elektronischer Zahlungsverkehr, Chipkarten, Internet, Sicherheitskriterien, Sicherheitskonzepte, Rollen- und aufgabenbasierte Zugriffsmodelle

*Publikationen aus dem Projekt (siehe Publikationsliste)*

## **2.5 Rollenbasierte Zugangskontrolle für das Hardwarelabor des Arbeitsbereiches AGN unter Verwendung von Chipkarten (NTC-SESAM)**

Nachdem Frau Dr. Schier die Universität Hamburg zwecks praktischer Tätigkeit bei einem Finanzinstitut verlassen hat, wird dieses Projekt im Rahmen von studentischen Examensarbeiten sowie von Doktorarbeiten fortgeführt.

Gegründet von: Schier, K., Dipl.-Inform.

*Laufzeit des Projektes:*

09/95 – 07/99

*Projektbeschreibung:*

Im Rahmen eines studentischen Projektes wurde ein Zugangskontrollsystem entwickelt, das den Zugang zum AGN-Labor und zu den PCs regelt. NTC-SESAM steht für Netz Test Center- Security enhanced System for Access Management (das Akronym soll an das märchenhafte „Sesam öffne Dich“ anknüpfen). Das Kontrollsystem wurde nach einem rollenbasierten Zugriffsmodell entwickelt, das den Nutzern des Systems spezifische Rollen zuordnet, nach denen sich der Zugang ergibt. Die Realisierung erfolgte auf der Basis von Chipkarten. Es wurde ein universeller Chipkartenleser gebaut, der im Projekt verwendet wird, um verschiedene Arten von Karten lesen zu können. Den Benutzern des Systems werden verschiedene Rollen zugeordnet, nach denen sie Zugang zu den unterschiedlichen Bereichen des Arbeitsbereiches, später auch des Fachbereichs haben. Als Erweiterungen sind der Zugang zu Rechnern, eventuell auch Mensakarten o.ä. geplant. Eine erste Demonstration der Funktionsfähigkeit erfolgt an einem Modell auf den Hamburger Computertagen 1998/1999.

*Schlagwörter:*

Rollenbasierte Zugangskontrolle, Chipkarten, Internet, Sicherheitskriterien, Sicherheitskonzepte

*Publikationen aus dem Projekt:*

Pflichtenheft zum Projekt NTC-SESAM <http://agn-www.informatik.uni-hamburg.de/>,  
unter: → Projekte → Chipkarten Projekt

## **2.6 Rollenbasierte Zutritts- und Rechnerzugangskontrolle für das AGN-Projektlabor unter Verwendung von Identifikationsverfahren der Biometrie (NTC-RAMSeS)**

Brömme, Arslan

*Laufzeit des Projektes:*

10/1999 - 10/2002

*Projektbeschreibung:*

Im Rahmen des Projektes NTC-RAMSeS (Role-Based Access Management Security System) wird ein auf Identifikationsverfahren der Biometrie gestütztes Kontrollsystem entwickelt, das den Zutritt zum AGN-Projektlabor und den Zugang zu den Projektrechnern regelt.

Das Projekt wird mit Hilfe von Studierenden im AGN-Forschungsschwerpunkt unter Anleitung von Arslan Brömme durchgeführt. Jeweils zum Semesterende wird eine Projektdokumentation erstellt, die durch zwischenzeitliche Fortschrittsberichte ergänzt wird. Im Rahmen von RAMSeS wurde eine digitale Kamera für die ersten Tests zur Iriserkennung angepaßt. Den Systembenutzern sollen unter RAMSeS verschiedene Rollen zugeordnet werden, mit denen sie entsprechenden Raum- und Systemzugang haben. Die Erweiterungen des Projektes betreffen die Anwendbarkeit weiterer biometrischer Identifikationsverfahren (z.B. Gesichtserkennung) und die Entwicklung eines Managementsystems zur Authentisierung seinerseits schutzwürdiger biometrischer Signaturen. Die Entwicklung von RAMSeS erfolgt unter Windows NT mit geeigneten digitalen Kameras und Videokarten. Eine Demonstration ist für die Hamburger Computertage HCT 2001 vorgesehen.

Im Berichtsjahr wurden neben einem Rahmensystem für biometrische Authentifikation auch verschiedene Klassen von Algorithmen zur Verarbeitung biometrischer Muster insbesondere für die Iris-Biometrie entwickelt (Doktorarbeit A. Brömme).

*Schlagwörter:*

Rollenbasierte Zugangskontrolle, Identifikationsverfahren der Biometrie, Sicherheitskonzepte, rollenbasierte Zugriffsmodelle, Sicherheitsmodelle

## **2.7 Rechtliche und Gesellschaftliche Aspekte der Informationsgesellschaft, Computer-Ethik**

Brunnstein, Klaus, Prof. Dr.

*Projektbeschreibung*

Im Rahmen internationaler Kooperation werden Wirkungen des Einsatzes informatischer Techniken und Methoden untersucht. Vor allem durch Vernetzung entstehen teilweise einschneidende Veränderungen heutiger Arbeitsformen, Berufe, Geschäftsfelder bis hin zu staatlichem und gesellschaftlichem Handeln.

In den letzten Jahren wurden schwerpunktmäßig die gesellschaftlichen Risiken und rechtlichen Aspekte (u.a. Datenschutzprobleme, Computerkriminalität, intellektuelle Eigentumsrechte/Urheberschutz) der „Globalen Informationsgesellschaft“ untersucht. In internationaler Kooperation (IFIP TC-9) wurde ferner an einer Analyse von Ethischen Kodizes verschiedener Informatikorganisationen leitend mitgearbeitet.

*Schlagwörter:*

Technologiefolgenabschätzung, Datenschutz, Computerkriminalität, Globale Informationsgesellschaft, NII, Computer-Ethik

*Publikationen aus dem Projekt (siehe Publikationsliste)*

## **2.8 Nachanalysen (Phase 2) zum "Jahr 2000"-Problem**

Brunnstein, Klaus, Prof. Dr.

*Laufzeit des Projektes:*

1998 – 1999, 2000-2001

*Projektbeschreibung:*

Während in der Vorphase (bis 31.12.1999) die Analyse und Vermeidung von Jahr-2000 Risiken im Vordergrund stand – hierzu gab es ein Projekt mit der Handelskammer Hamburg, innerhalb dessen Projekts Studenten zu Y2k-Fachleuten ausgebildet wurden – steht in der zweiten Phase die Analyse von tatsächlich eingetretenen Wirkungen sowie von Spätfolgen im Vordergrund. Weil zahlreiche tatsächlich eingetretenen Vorfälle gezielt verheimlicht wurden, tauchen Fakten gelegentlich in gänzlich anderem Zusammenhang auf (siehe reports in Risk Forum der ACM).

*Schlagwörter:*

Jahr-2000-Problem, Millennium Bug, Y2k, Wirkungen, Spätfolgen

## **2.9 Testverfahren für die Angriffsstabilität von Firewalls**

Kassovic, Marian, Dipl.-Inform.

*Laufzeit des Projektes:*

08/98 – 30.04.2001

Anmerkung: nach seinem Ausscheiden (am 30.4.2001) bearbeitet Herr Kassovic dieses Thema weiter im Rahmen seiner nunmehr extern durchgeführten Doktorarbeit.

*Projektbeschreibung:*

Firewalls stellen einen wirkungsvollen Schutzmechanismus bei der Vernetzung von Rechensystemen insbesondere bei der Kopplung von LANs bzw. deren Anbindung an das Internet dar. Eine Firewall soll ein Netzwerk gegen Angriffe von außen schützen, ohne dabei den Netzverkehr von innen zu stark einzuschränken. Zur Umsetzung der in einer Security Policy formulierten Anforderungen an die Firewall kommen Filter und Proxies zum Einsatz.

Cracker versuchen die von der Firewall auferlegten Beschränkungen auszuschalten oder zu umgehen. Zur Beurteilung der Angriffsstabilität einer Firewall müssen geeignete Testverfahren entwickelt werden, die eine Überprüfung der Wirksamkeit der implementierten Schutzmaßnahmen erlauben. Innerhalb des Projekts erfolgt eine praktische Erprobung derartiger Verfahren an der Linux-basierenden Firewall des Arbeitsbereichs.

*Schlagwörter:*

Firewall, Penetration Testing, Angriffsstabilität

*Publikationen aus dem Projekt (siehe Publikationsliste)*

***Drittmittelprojekte***

Brunnstein, Klaus, Prof. Dr.; Kassovic, Marian, Dipl.-Inform. (bis 30.04.2001)

**2.10 ERASMUS/SOKRATES -Programm „IT Security & Safety Education“ (29770-IC-1-96-1-DE-ERASMUS-EPS-1), „European Graduate on Security of Information and Communication Systems“ (29118-IC-1-96-GR-ERASMUS-EPS-1)**

*Laufzeit:*

von Oktober 1995 bis Oktober 1996 (ICP-95-G-4016/11),

von Oktober 1996 bis Oktober 1997 (ICP-96-G-4016/11)

von Oktober 1997 bis Oktober 1998 (29770-IC-1-96-1-DE-ERASMUS-EPS-1, 29118-IC-1-96-GR-ERASMUS-EPS-1)

von Oktober 1998 bis Oktober 1999 (29118-IC-2-97-1-GR-ERASMUS)

von Oktober 1999 bis Oktober 2001 (29118-IC-3-98-1-GR-ERASMUS)

*Projektbeschreibung:*

An diesem Kooperationsprojekt sind 20 Universitäten aus 11 verschiedenen europäischen Ländern beteiligt, die ihre Studenten in IT-Sicherheit ausbilden (siehe oben unter „Wissenschaftliche Zusammenarbeit“). Durch dieses Erasmus/Sokrates-Programm wird der Studenten- und Dozentenaustausch zwischen den beteiligten Universitäten gefördert. Zudem wird eine gemeinsame Erarbeitung von Kursmaterialien und Lehrplänen für Curricula in IT-Sicherheit gefördert. Bisher wurde ein Vorschlag für ein Curriculum in „Information Security, Dependability and Safety“ für europäische Universitäten erarbeitet. Im Rahmen der CDA („Curriculum Development Activity“-)Maßnahme „European Graduate on Security of Information and Communication Systems“ wird zur Zeit an einer Zusammenstellung von elektronischen Kursmaterialien für ein solches Curriculum und Konzepten für ein „Distance Learning“-Angebot in dem Fachgebiet gearbeitet.

*Finanzierung:*

Geldgeber:	EU
Laufzeit der Förderung:	10/1994 - 10/2000
Sachmittel:	7.650 ECU

**2.11 Referenzstelle für Basisdatendokumentation**

Brunnstein, Klaus, Prof., Dr.; Kassovic, Marian, Dipl.-Inform. (bis 30.04.2001)

*Laufzeit des Projektes:*

Dezember 1997- 2002

*Projektbeschreibung:*

Unabhängige Referenzstelle für die Errichtung, Verwaltung und Durchführung einer für Hamburg zentralen Erfassung von (anonymisierten) Datensätzen im Rahmen der Basisdatendokumentation im ambulanten Sucht- und Drogenhilfesystem mit dem Ziel der Erfassung und Zuordnung von Mehrfachmeldungen.

*Finanzierung:*

Geldgeber:	BADO e.V.
Sach- und Personalmittel:	ca. 5.400 DM/12.000 DM

### 3. Publikationen und weitere Leistungen

#### Wissenschaftliche Publikationen (seit 1995):

AB AGN: zahlreiche Publikationen (VTC Tests, Dokumentationen etc; Artikel/Beiträge; Studien/Bachelor/Diplomarbeiten) auf den Internet-Seiten des Arbeitsbereiches:

<http://agn-www.informatik.uni-hamburg.de/vtc>

- Brunnstein, K., Sint, P. (Herausgeber): Intellectual Property Rights and New Technologies, Proceedings of the KnowRight'95 Conference, Wien, August 1995, Schriftenreihe der Österreichischen Computer Gesellschaft, R.Oldenbourg, 1995
- Brunnstein, K., Fischer-Hübner, S.: How far can the criminal law help to control IT-Misuse ?, in: *The 1995 Yearbook of Law, Computers and Technology*, Hrsg.: Martin Wasik Vol.9, Carfax, 1995
- Berleur, J., Brunnstein, K. (Herausgeber): Ethics of Computing - Codes, Spaces for Discussion and Law, Chapman & Hall, 1996.
- Brunnstein, K.: Technische Risiken und ihre möglichen Wirkungen auf dem Wege in eine 'Informationsgesellschaft', in: Britta Schinzel (Hrsg.) , „Schnittstellen - Studien zum Verhältnis zwischen Informatik und Gesellschaft“, Vieweg-Verlag, 1996
- Brunnstein, K., Schier, K.: Global Digital Commerce: Impacts and Risks for Developments of Global Information Societies, in: J.Berleur and Diane Whitehouse, Hrsg., 'An ethical global information society: culture and democracy revisited', Proceedings of the IFIP WG 9.2 Corfu international conference, 8.-10. Mai 1997, Chapman&Hall, 1997.
- Fischer-Hübner, S.: Privacy at Risk in the Global Information Society, in: J.Berleur and Diane Whitehouse, Hrsg., 'An ethical global information society: culture and democracy revisited', Proceedings of the IFIP WG 9.2 Corfu international conference, 8.-10. Mai 1997, Chapman&Hall, 1997.
- Klaus Brunnstein: „Protecting Access in LANs, C/S-Systems and IntraNets“, Tagungsband SecureNet96, North Holland/Elsevier (1996)
- Klaus Brunnstein: Wie sicher ist die Informationstechnik Deutscher Banken?, Business Computing: Sonderheft Banken (Juni 1996)
- Klaus Brunnstein: „Ist Wirtschaften im Internet zu riskant? Über Sicherheitsrisiken und Schutzmaßnahmen im Internet“, Business Computing (Juli 1996)
- Klaus Brunnstein: „Über die Beherrschung Technischer Risiken der Informationsgesellschaft“, Tagungsband 50. Deutscher Betriebswirtschafter-Tag (1996)
- Klaus Brunnstein: „From 10 to 10,000 Viruses: IFIPs Involvement in Fighting Malicious Software“, in: IFIP 25 Years Review, Heinz Zemanek (Editor), North Holland (1996)
- Klaus Brunnstein: „LAN Access Controls & Authentication“, Tagungsband SecureNet'96, North Holland/Elsevier, 1996
- Klaus Brunnstein: „Java: Security and Safety Aspects“, Tagungsband Compsec96, North Holland/Elsevier, 1996
- Klaus Brunnstein: „Beyond Computer Viruses:Malicious Agents, Hostile Applets and More Emerging Malicious Software in IntraNets and Internet“, EICAR-Tagungsband, 1996
- Brunnstein, K., Schier, K., Global Digital Commerce: Impacts and Risks for Developments of Global Information Societies“, in: J.Berleur and Diane Whitehouse, Hrsg., 'An ethical global information society: culture and democracy revisited', Proceedings of the IFIP WG 9.2 Corfu international conference, 8.-10. Mai 1997, Chapman&Hall, 1997.

- Klaus Brunnstein: „Threats to Individual Privacy and Enterprise Security and Experiences with Internet InSafety and InSecurity“ Tagungsband „InfoEthics“, UNESCO, 1997
- Klaus Brunnstein: „Towards an Holistic View of Enterprises ICT Security and Safety“, Tagungsband International Information Security Conference (IFIP/SEC'97), North Holland/Elsevier, 1997
- Klaus Brunnstein: „Determining the Quality of Anti-Virus and Anti-Malware Products“, Information Security Bulletin (November 1997)
- K. Brunnstein, K. Schier: Sicherheitsrisiken beim Online-Banking, GI Geldinstitute, Heft 11-12, Dezember 1997, Hans Holzmann Verlag, Bad Wörishofen, 1997, S. 64-66
- Klaus Brunnstein, Till Teichmann u.a.: „AntiVirus Product Test 1997-02“, Homepage AB AGN
- Klaus Brunnstein, Till Teichmann u.a.: „AntiVirus Product Test 1997-07“, Homepage AB AGN
- Klaus Brunnstein; Kathrin Schier: „Über Risiken Computer- und Netz-gestützter Bankanwendungen Fachzeitschrift Geldinstitute“, Holzmann-Verlag, Dezember 1997
- Klaus Brunnstein: „Internet - Freiheit oder Gläserner Mensch?“, Tagungsband Goethe-Institut Luxemburg, 1998
- Brunnstein, K., Fischer-Hübner, S., Schaar, P.: "Verbraucherbefragung" & "Globale Informationsgesellschaft", in: Computer und Recht aktuell, Computer und Recht, Feb. 1998, Verlag Dr. Otto Schmidt
- Klaus Brunnstein: zahlreiche Vorträge und Beiträge zu Tagungsbänden bei internationalen Konferenzen (1995-2001)
- Fischer-Hübner, S.: Towards a Privacy-Friendly Design and Usage of IT-Security Mechanisms, in: Proceedings of the 17th National Computer Security Conference, Baltimore MD, Oktober 1994.
- Fischer-Hübner, S.: Considering Privacy as a Security-Aspect: A Formal Privacy-Model, DASY-Papers No. 5/95, Institute of Computer and System Sciences, Copenhagen Business School, 1995.
- Sobirey, M., Fischer-Hübner, S.: Privacy-Oriented Auditing, in: Proceedings of the CSR (Centre for Software Reliability) 13th Annual Workshop on „Design for Protecting the User“, Bürgenstock, Schweiz, 11.-13. September, 1996.
- Fischer-Hübner, S., Schier, K.: Der Weg in die Informationsgesellschaft - Eine Gefahr für den Datenschutz, in: Britta Schinzel (Hrsg.), „Schnittstellen - Studien zum Verhältnis zwischen Informatik und Gesellschaft“, Vieweg-Verlag, 1996
- Fischer-Hübner, S., Schier, K.: Risks on the Way to the Global Information Society, in: Proceedings of the IFIP-TC-11 Sec'96-Conference, Samos, Mai 1996, Hrsg.: S.Katsikas, D.Gritzalis, Chapman & Hall.
- Fischer-Hübner, S.: Privacy at Risk in the Global Information Society, in: J.Berleur and Diane Whitehouse (Hsg.), 'An ethical global information society: culture and democracy revisited', Proceedings of the IFIP WG 9.2 Corfu international conference, 8.-10. Mai 1997, Chapman&Hall, 1997.
- Sobirey, M., Fischer-Hübner, S., Rannenber, K.: Pseudonymous Auditing for a Privacy-Enhanced Intrusion Detection, in: Proceedings of the IFIP TC-11 Sec'97-Conference „Information Security in Research and Business“, Kopenhagen, 14.-16. Mai 1997, Hrsg.: L.Yngstroem, J.Carlsen, Chapman&Hall, 1997
- Fischer-Hübner, S.: A Formal Task-based Privacy Model and its Implementation: An updated Report, in: Proceedings of the Second Nordic Workshop on Secure Computer Systems NORDSEC'97, Hrsg.: A.Karila, T.Aalto, Helsinki, 6.-7. November, 1997.

- Simone Fischer-Hübner, Gerald Quirchmayr, Louise Yngström (Hrsg.), Proceedings of the IFIP WG 8.5 / 9.6 Working Conference "User Identification and Privacy Protection - Applications in Public Administration and Electronic Commerce", 14-15 Juni 1999, Department of Computer and System Sciences (DSV), Stockholm University/ KTH, DSV-Report Series 99-007
- Louise Ynström, Simone Fischer-Hübner (Hrsg.), Proceedings of the IFIP WG 11.8 1st World Conference on Information Security Education (WISE1), 17.-19. Juni 1999, Department of Computer and System Sciences (DSV), Stockholm University/ KTH, DSV-Report Series 99-008
- Fischer-Hübner, S. : Privacy-Enhancing Design and Use of IT-Security Mechanisms, Habilitationsschrift, Fachbereich Informatik,, Universität Hamburg, Juli 1999 <MO>
- Fischer-Hübner, S.: Datenschutz durch Technik, eingeladener Beitrag zur Herbsttagung der Mathematischen Gesellschaft in Hamburg, 5.11.1999, zur Veröffentlichung in: Mitteilungen der Mathematischen Gesellschaft in Hamburg, Band XIX, 2000 <nDT>
- Marian Kassovic, Ole Marienhagen, Jens Nedon: Angriffsstabilität der AGN-Firewall, Projektdokumentation 1998/99
- Ott, A.: Regelsatzbasierte Zugriffskontrolle nach dem „Generalized Framework for Access Control“-Ansatz am Beispiel Linux, Diplomarbeit, Fachbereich Informatik, Universität Hamburg, November 1997.
- Ott, A. : Rule Set Based Access Control (RSBAC), <http://www.rsbac.de/rsbac/>
- Schier, K: Vergleich und Bewertung aktueller Systeme im elektronischen Zahlungsverkehr, Proceedings der German Unix User Group Jahrestagung GUUG '97, Wiesbaden, 16-18 September 1997
- Schier, K: Sicherheitsaspekte des Einsatzes von Chipkarten in sensitiven Anwendungen, ENCRESS-Tagung, Tagungsband, April 1996.
- K. Schier, Brunstein, K., Global Digital Commerce: Impacts and Risks for Developments of Global Information Societies", in: J.Berleur and Diane Whitehouse, Hrsg., 'An ethical global information society: culture and democracy revisited', Proceedings of the IFIP WG 9.2 Corfu international conference, 8.-10. Mai 1997, Chapman&Hall, 1997.
- K. Schier, A. Engel, A. Lessig: Kartengestützter Zahlungsverkehr - Der Große Bruder im Portemonnaie, Proceedings der OmniCard '98, 14-16 Januar 1998, InTime, Berlin, 1998, S.19-43
- K.Schier: Sicherheitsaspekte aktueller Systeme im elektronischen Zahlungsverkehr, Offene Systeme', Zeitschrift deutschsprachiger Unix-Benutzer-Vereinigungen, Band 7, Nr.1, Februar 1998, Springer, 1998, ISSN 0941 1968, S. 19-26
- K.Schier: Zahlungssysteme im Internet - Eine sicherheitstechnische Bewertung, in: Heinen, I. (Hrsg): Internet - von der Idee zum kommerziellen Einsatz, Deutscher Internet Kongreß, Frankfurt, dpunkt.verlag Mai 1998, ISBN 3 932588 20 7, S. 223-233
- K. Schier, S. Fischer-Hübner: The Global Information Society and electronic Commerce: Privacy Threats and Privacy Technologies, Proceedings der IFIP Fifth World Conference Human Choice and Computers, Computers and Networks in the Age of Globalization, 25-28 August 1998, S. 503-515
- K.Schier: A role and task based Security Model for mutlifunctional smartcard application in the area of electronic commerce, Proceedings der IFIP/SEC'98, Wien, Budapest 31.08.98 - 04.09.98, Schriftenreihe der Österreichischen Computergesellschaft, Band 116, ISBN 3 85403 116 5, 1998, S. 219-229

- K. Schier: Multifunctional Smartcards for electronic commerce- Appliaction of the role and task based security model, Proceedings of the Annual Computer Security Application Conference ACSAC 1998, 7-11.Dezember 1998, Phoenix, ISBN 0 8186 8789 4, 1998, S. 147-154
- K.Schier: Der autonome Kunde im Vordergrund - Freie Wahl der Zahlungsmodalität bei multifunktionalen Chipkarten, Proceedings der OmniCard '99, 13.-15. Januar 1999, InTime, Berlin, 1999
- Schier, K.: Sicherheit elektronischer Zahlungssysteme im Internet, in: Krallmann, H. Scholz-Reiter, B. (Hrsg.): Industrie Management - Electronic Commerce, 15. Jahrgang, Ausgabe 1/1999, GITO-Verlag für Industrielle Informationstechnik und Organisation GmbH, Berlin, Februar 1999
- Schier, K.: Vertrauenswürdige Kommunikation im elektronischen Zahlungsverkehr - Ein Rollen- und Aufgabenbasiertes Sicherheitsmodell für Anwendungen mit multifunktionalen Chipkarten, Dissertation am Fachbereich Informatik der Universität Hamburg, Hamburg, Juni 1999

### Abgeschlossene Doktorarbeiten

DoktorandIn	BetreuerIn	Thema	Datum
Klaus-Peter Kossakowski	K. Brunnstein	Foundations of Incident Response Methods	Summer 2001
Prague: Suzana Celustka-Stojakovic	Klaus Brunnstein	Building Secure Information Systems	April 2001, Prague

### Abgeschlossene Diplomarbeiten (DiplomPrüfungsOrdnung von 1985)

DiplomandIn	BetreuerIn	Thema	Datum
Claudius Haasis	J.W. Schmidt K. Brunnstein	Referenzmodelle für Standardsoftware: Anforderung, Nutzung und methodische Grundlagen	Januar 2001
Frank Ruschmeyer	K.Brunnstein Hans-Joachim Mück	Verfahren und Techniken zur Verfolgung von Computer- und Cyberkriminalität mit Methoden der Forensischen Informatik	März 2001
Sibel Mutlu, Axel Schnell, Emine Yüksel	K. Brunnstein S.Fischer-Hübner	Intrusion Detection als ergänzender Mechanismus am Beispiel von UNIX	März 2001
Christoph Haas	K. Brunnstein Hans-Joachim Mück	Sicherheitsmanagement für UNIX-Server am Modell eines verteilten Unternehmensnetzwerkes	Juni 2001
Tanja Hofmann	K. Brunnstein Hans-Joachim Mück	E-Business Sicherheit: Methoden, Probleme und Lösungsansätze unter Berücksichtigung von Public Key Infrastrukturen und digitalen Signaturen	Juli 2001
Hartmut Irrgang	Hans-Joachim	Erkennung von Einbrüchen in	August

	Mück K. Brunnstein	Netzwerke	2001
--	-----------------------	-----------	------

#### Abgeschlossene Studienarbeiten (Diplomprüfungsordnung von 1985)

StudienarbeiterIn	BetreuerIn	Thema	Datum
Michael Stradt	K. Brunnstein	Konzeptionelle Migration einer FoxPro-Datenbank an das WorldWideWeb	Januar 2001
Andre Lürssen	K. Brunnstein	Netzprogrammierung mit Java2: Risiken und Lösungsansätze	Februar 2001
Kai Dittberner, Marc Poli	K. Brunnstein	Sicherheitslücken von Microsoft Windows 2000 und Gegenmaßnahmen	August 2001
Gabriel Ngatchui	K. Brunnstein	Spezielle Aspekte des Jahr-2000 Problems in Afrika (dargestellt am Beispiel von Kamerun)	November 2001

#### Abgeschlossene Bachelorarbeiten (Diplomprüfungsordnung von 1998)

StudienarbeiterIn	BetreuerIn	Thema	Datum
Benjamin Hoherz, Silvio Krüger, Jan Menne, Nils Michaelsen	K. Brunnstein	Internet-Telefonie: Eine sinnvolle Ergänzung zu herkömmlicher Telefonie im Unternehmen und Privathaushalt? Technologie, Produkte, Sicherheit und Kosten	Juli 1999

#### 4. Wichtige weitere Aktivitäten

##### Mitarbeit in wissenschaftlichen außeruniversitären Gremien

Klaus Brunnstein:

Deutscher Vertreter in der Generalversammlung (General Assembly) der International Federation for Information Processing (IFIP) seit 1999

Vice President der IFIP (seit September 2000)

Vorsitzender des IFIP-Beirates der deutschen Informatik-Fachgesellschaften (u.a. Gesellschaft für Informatik, GI; Informationstechnische Gesellschaft ITG im VDE; Deutsche Physikalische Gesellschaft, DPG)

Deutscher Vertreter in IFIP TC-9 „Relationship between Computers and Society“ (Chair TC-9: 1990-1995)

Mitglied WG 9.2 „Social Accountability“ und SIG 9.2.2 „Computer Ethics“

Mitglied des Präsidiums der Gesellschaft für Informatik (GI): (1996-1998, 1999-2001)

Vorsitzender und Mitglied mehrerer International Program Committees

Marian Kassovic, Klaus Brunnstein:

Referenzstelle für die Basisdatendokumentation

Betreuung der Erasmus-Studenten

Arslan Brömme:

Mitglied IFIP WG 9.6 „Computer Misuse and the Law“

**Mitarbeit in wissenschaftlichen universitären Gremien**

Klaus Brunnstein:

Vorsitzender des Prüfungsausschusses Informatik

Datenschutz-Beauftragter des FB Informatik

Arslan Brömme:

Mitglied der Berufungskommission "C4-Professur IT-Sicherheit und Datenschutz"

Stv. Datenschutz-Beauftragter des FB Informatik

Marian Kassovic:

Stv. Mitglied der Berufungskommission "C4-Professur IT-Sicherheit und Datenschutz"

Mitglied des Umweltteams



