Beschlussvorlage

zur GI-Präsidiumssitzung
31. Januar / 1. Februar 2002

zu TOP 12

Antragsteller:

GI-Fachgruppe 2.0.2/2.5.3 Verlässliche IT-Systeme (VIS)
vertreten durch die Sprecherin: Marit Köhntopp

GI-Fachgruppe 3.6.1 Fehlertolerierende Rechensysteme
vertreten durch den Sprecher: Karl-Erwin Grosspietsch

GI-Fachgruppe 3.6.2 ENCRESS
vertreten durch die Sprecherin: Francesca Saglietti

GI-Fachgruppe 2.1.5 ADA
vertreten durch den Sprecher: Peter Dencker

Gründung des GI-FB „Sicherheit – Schutz und Zuverlässigkeit“

Sehr geehrte Damen und Herren,

zur Präsidiumssitzung am 29./30. Juni 2001 hat das Präsidium der GI auf Antrag einer Initiativgruppe beschlossen, die Gründung eines neuen Fachbereichs mit der inhaltlichen Ausrichtung auf die Themen Sicherheit, Schutz und Zuverlässigkeit informatischer Systeme voranzutreiben. Durch das Präsidium wurden hierfür Auflagen mitgegeben, die für die angestrebte Gründung im Januar 2002 erfüllt werden sollen.

Die Initiativgruppe hatte seinerzeit einen detaillierten Antrag vorgelegt, der eine mögliche inhaltliche Positionierung dieses Themas innerhalb der GI sowie eine mögliche Untergliederung umfasst. Zum damaligen Zeitpunkt bestand noch Klärungsbedarf in einigen organisatorischen Punkten, wobei einige dieser Punkte zu einer grundsätzlichen Diskussion innerhalb der GI führten, die auf Ebene des Präsidiums zu leisten war. Innerhalb des Präsidiums ist unter Beteiligung der Antragsteller die Diskussion vorangeschritten und die Diskussionsergebnisse sind in dem vorliegenden Antrag berücksichtigt.

Die Initiativgruppe hat ihrerseits die offenen Punkte geklärt und stellt nunmehr den Antrag auf Einrichtung des Fachbereichs mit dem Titel „Sicherheit – Schutz und Zuverlässigkeit“. Der Fortschritt gegenüber dem Antrag zur Sitzung im Juni 2001 lässt sich wie folgt kurz darstellen:

- Der Kreis der Antragsteller hat sich vergrößert auf nunmehr 4 bestehende GI-Fachgruppen aus unterschiedlichen Fachbereichen der GI.
- Es wurde zwischen den in der GI bestehenden Safety- und der Security-„Communities“ ein inhaltlicher Konsens erzielt, den neuen Fachbereich gemeinsam zu gestalten.
- Es bestehen konkrete Planungen für die ersten Veranstaltungen des FB, für Kooperationen mit weiteren Fachbereichen der GI sowie für Kooperationen mit befreundeten Organisationen, z.B. der ITG-Fachgruppe „IT-Sicherheit“ und der Fachgruppe IT-Security der Schweizer Informatikgesellschaft.
- Der Fachbereich vertritt ausreichend viele Mitglieder, um sich innerhalb der GI gegenüber anderen Fachbereichen positionieren zu können.
- Es wird ein Leitungsgremium vorgeschlagen, das für den Startzeitraum von 3 Jahren den Aufbau des FB organisieren soll.

Es besteht ein starkes Interesse, nach Einrichtung des Fachbereichs neue Fachgruppen zu gründen, um den FB inhaltlich auszudifferenzieren. Diese FGs können gemäß GOGL jedoch erst nach Einrichtung des FB durch diesen gegründet werden; die Vorbereitungen hierfür sind jedoch weitestgehend abgeschlossen. Auch hier gibt es sehr viele Interessente. Die inhaltliche Ausgestaltung obliegt dann dem FB. In diesem Antrag wird die geplante Struktur dargestellt.

Inhaltsverzeichnis

1 Beschlussantrag

Das Präsidium der Gesellschaft für Informatik e.V. möge beschließen:

Teilbeschluss 1: FB-Einrichtung

Das Präsidium beschließt die Einrichtung eines neuen GI-Fachbereichs mit dem Titel „Sicherheit“ und dem Untertitel „Schutz und Zuverlässigkeit“.

Teilbeschluss 2: FB-Leitungsgremium

Das Präsidium setzt gemäß GOGL das folgende vorläufige Leitungsgremium ein:

Sprecher:

- Manfred Reitenspieß manfred@reitenspiess.de

Stellvertretende Sprecher:

- Isabel Münch muench@bsi.de
- Jens Nedon nedon@consecur.de

Weitere Mitglieder des Leitungsgremiums:

- Ammar Alkassar
- Wolfgang Behnsen
- Fevzi Belli
- Arslan Brömme
- Frank Damm
- Hannes Federrath
- Dirk Fox
- Rüdiger Grimm
- Karl E. Großpietsch
- Patrick Horster
- Matthias Jänichen
- Jan Jürjens
- Hubert B. Keller
- Klaus Keus
- Marit Köhntopp
- Klaus-Peter Kossakowski
- Günther Pernul
- Andreas Pfitzmann
- Kai Rannenberg
- Peer Reymann
- Francesca Saglietti
- Hans von Sommerfeld
- Helmut Stiegler
- Gerhard Weck
- Petra Wohlmacher

Teilbeschluss 3: Zuordnung von Fachgruppen

Das Präsidium beschließt die anfängliche Zuordnung von folgenden Fachgruppen zum neuen Fachbereich Sicherheit:

- Fachgruppe VIS (bisher 2.0.2/2.5.3) als alleinige Zuordnung zum FB Sicherheit (d.h. gleichzeitige Aufhebung der bestehenden Zuordnungen zu den FB 2 (Softwaretechnik) und FB DBIS,
- Fachgruppe 3.6.1 Fehlertolerierende Rechensysteme als zusätzliche Zuordnung zum FB Sicherheit,
- Fachgruppe 3.6.2 ENCRESS als zusätzliche Zuordnung zum FB Sicherheit,
- Fachgruppe 2.1.5 ADA als zusätzliche Zuordnung zum FB Sicherheit.

Die einzelnen Punkte des Antrags werden nachfolgend detailliert begründet

1.1 Begründung zu Punkt 1 des Beschlussantrags

> Das Präsidium beschließt die Einrichtung eines neuen GI-Fachbereichs mit dem Titel „Sicherheit“ und dem Untertitel „Schutz und Zuverlässigkeit“.

Begründung:

Der Antrag wird begründet mit der aufstrebenden Entwicklung dieses Fachgebietes, in dem eine querschnittliche Behandlung vieler Themen aus der Informatik und aus angrenzenden Fachgebieten erfolgt. Sowohl im wissenschaftlichen als auch im wirtschaftlichen Bereich spielt dieses Thema eine rasant wachsende Rolle. Die GI äußert sich nach außen gelegentlich zu diesem Thema, sichtbare Möglichkeiten der Mitarbeit an diesem Thema innerhalb der GI bestehen jedoch für Mitglieder nur in sehr eingeschränktem Maße: unter den für Teilbereiche (Kommunikationssicherheit, Security, Dependability, Datenschutz) bestehenden Fachgruppen findet fast keine Quervernetzung statt, und viele, aus einer ganzheitlichen Betrachtung des Themas resultierende Gebiete, z.B. ethischer, rechtlicher und organisatorischer Natur sind unterrepräsentiert.

Wir wollen das ändern und dem Thema „Sicherheit“ unter den Aspekten Schutz sowie Zuverlässigkeit informatischer Systeme eine starke Sichtbarkeit in der GI und darüber hinaus verschaffen. Mit Hilfe eines Fachbereiches zu diesem Thema wollen wir den an dieser Thematik beteiligten Fachgruppen, insbesondere auch den in diesem Gebiet arbeitenden Informatikern, ein Forum bieten, in dem sie ihr Fachthema, organisiert in Fachgruppen, wiederfinden.

Der geplante Aufbau, der natürlich erst nach Einrichtung des Fachbereichs durch diesen selbst umgesetzt werden muss, ist in den nachfolgenden Abschnitten detailliert dargestellt.

1.2 Begründung zu Punkt 2 des Beschlussantrags

Das Präsidium setzt gemäß GOGL ein vorläufiges Leitungsgremium ein, das aus folgenden Personen besteht:

Sprecher:

- Manfred Reitenspieß	manfred@reitenspiess.de

Stellvertretende Sprecher:

- Isabel Münch	muench@bsi.de
- Jens Nedon	nedon@consecur.de

Weitere Mitglieder des Leitungsgremiums:

- Ammar Alkassar	alkassar@cs.uni-sb.de
- Wolfgang Behnsen	Wolfgang.Behnsen@t-systems.de
- Fevzi Belli	belli@sigma.uni-paderborn.de
- Arslan Brömme	broemme@informatik.uni-hamburg.de
- Frank Damm	Frank.F.Damm@bku.db.de
- Hannes Federrath	federrath@inf.tu-dresden.de
- Dirk Fox	fox@secorvo.de
- Rüdiger Grimm	ruediger.grimm@tu-ilmenau.de
- Karl E. Großpietsch	grosspietsch@gmd.de
- Patrick Horster	Patrick.Horster@t-online.de
- Matthias Jänichen	mj@percomp.de
- Jan Jürjens	juerjens@informatik.tu-muenchen.de
- Hubert B. Keller	keller@iai.fzk.de
- Klaus Keus	klaus.keus@bsi.bund.de
- Marit Köhntopp	marit@koehntopp.de
- Klaus-Peter Kossakowski	Klaus-Peter@kossakowski.de
- Günther Pernul	pernul@wi-inf.uni-essen.de
- Andreas Pfitzmann	pfitza@inf.tu-dresden.de
- Kai Rannenberg	kair@microsoft.com
- Peer Reymann	pr@itqs.de
- Francesca Saglietti	saglietti@informatik.uni-erlangen.de
- Hans von Sommerfeld	IT-Sicherheit@t-online.de
- Helmut Stiegler	helmut.stiegler@sti-consulting.de
- Gerhard Weck	GerhardWeck@compuserve.com
- Petra Wohlmacher	petra.wohlmacher@regtp.de

Begründung:

Gemäß GOGL ist eine neue Untergliederung unter Benennung eines vorläufigen Leitungsgremiums einzusetzen. Dies erfolgt hiermit. Die Besetzung des Leitungsgremiums wurde unter den Initiatoren abgestimmt und erfolgt sowohl unter dem Kriterium der Arbeitsfähigkeit des Gremiums als auch unter einer möglichst repräsentativen und ausgewogenen Berücksichtigung der einzelnen Interessensgruppen unter den Initiatoren.

Die Benennung zweier Stellvertreter erfolgt unter dem Gesichtspunkt einer Zuarbeit zum Sprecher sowohl von formaler (FB-Organisation, finanzielle Fragen, etc.) als auch thematischer Seite (inhaltliche Koordination, Öffentlichkeitsarbeit, thematische Entwicklung des FB). Zusätzlich wurde berücksichtigt, dass die in der Startphase anfallende Arbeitslast (sowohl beim Aufbau des FB als auch seiner evtl. neuen Untergliederungen) möglichst breit verteilt wurde.

Die benannten Personen haben der Nominierung zugestimmt und ihre Bereitschaft zu aktiver Mitarbeit erklärt. Die hauptsächlichen Ansprechpartner werden nachfolgend kurz vorgestellt.

Vorstellung der Sprecher / Stellvertreter:

Manfred Reitenspieß

Manfred Reitenspieß ist seit Oktober 2000 bei Fujitsu Siemens Computers verantwortlich für technisches Marketing und Business Development des Resilient Telco Package (RTP). RTP unterstützt Integratoren und Middleware-Hersteller weltweit bei Design und Implementierung von hochverfügbaren Lösungen in den Segmenten Telekommunikation und E-Commerce. Davor war Manfred Reitenspieß in verantwortlicher Position zuständig für Entwicklung und Pflege von Produkten im Umfeld von Sicherheit, Verfügbarkeit und Kommunikation. Bis 1990 war er verantwortlich für die Implementierung der Personendosimetrie-Datenbank am CERN in Genf und war Systemarchitekt für fehlertolerante, sichere und verteilte Multiprozessorsysteme im Rahmen einer Kooperation zwischen Siemens und Intel, drei Jahre davon in Oregon, USA.

Manfred Reitenspieß promovierte 1983 an der Universität Erlangen-Nürnberg mit einer Arbeit zum Thema "Spezifikation und Implementation von Sicherheitsproblemen in Softwaresystemen". Er ist Gründungsmitglied der Fachgruppe Verlässliche Informationssysteme “VIS” der Gesellschaft für Informatik und war Mitorganisator nationaler und internationaler Workshops und Konferenzen für Sicherheit und Intelligente Netze. Er ist Inhaber von Patenten im Bereich der Konvergenz von Information und Kommunikation.

Kontaktinformation (für die GI-Datensammlung):

Fujitsu-Siemens Computers
Otto-Hahn-Ring 6 D-81739 München, Tel/Fax: ++49-89-636-42393, Email: manfred@reitenspiess.de

Isabel Münch

Isabel Münch hat Mathematik mit Nebenfach Informatik studiert. Nach dem Studium hat sie zunächst beim debis Systemhaus GEI als IT-Sicherheitsberaterin gearbeitet, seit 1994 ist sie Referentin im Referat Systemsicherheit und Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI). Dort ist sie Projektleiterin für die Weiterentwicklung des IT-Grundschutzhandbuches (Standardsicherheitsmaßnahmen für IT-Systeme).

Für das BSI ist sie in verschiedenen nationalen und internationalen Gremien tätig. Im Leitungsgremium der Fachgruppe VIS ist sie seit 1999. Sie soll als stellvertretender Sprecherin des Fachbereichs thematische Fragen des Fachbereichs bearbeiten und koordinieren.

Kontaktinformation (für die GI-Datensammlung):

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185, 53175 Bonn, Tel. ++49-228-9582-367, Fax: ++49-228-9582-405
Email: muench@bsi.de

Jens Nedon

Jens Nedon studierte Informatik mit dem Schwerpunkt „IT-Sicherheit“ und ist als Berater für IT-Sicherheit tätig. Er gehörte von 1996 bis 2001 dem Präsidium der Gesellschaft für Informatik als gewähltes Mitglied an und arbeitete dort u.a. in Arbeitskreisen mit, in denen formale Fragen der Präsidiums- und Gremienarbeit diskutiert wurden. Er ist daher bestens vertraut mit den organisatorischen Abläufen innerhalb der GI und soll als stellvertretender Sprecher des Fachbereichs organisatorische und formale Fragen des Fachbereichs koordinieren.

Kontaktinformation (für die GI-Datensammlung):

ConSecur GmbH
Schulze-Delitzsch-Straße 2, 49716 Meppen, Tel: 05931 / 9224-39 oder 0172 / 4049726,
Fax: 05931 / 9224-44, Email: nedon@consecur.de

1.3 Begründung zu Punkt 3 des Beschlussantrags

Das Präsidium beschließt die anfängliche Zuordnung von folgenden Fachgruppen zum neuen Fachbereich Sicherheit:

- Fachgruppe VIS (bisher 2.0.2/2.5.3) als alleinige Zuordnung zum FB Sicherheit (d.h. gleichzeitige Aufhebung der bestehenden Zuordnungen zu den FB 2 (Softwaretechnik) und FB DBIS,
- Fachgruppe 3.6.1 Fehlertolerierende Rechensysteme als zusätzliche Zuordnung zum FB Sicherheit,
- Fachgruppe 3.6.2 ENCRESS als zusätzliche Zuordnung zum FB Sicherheit,
- Fachgruppe 2.1.5 ADA als zusätzliche Zuordnung zum FB Sicherheit.

Begründung:

Die FG VIS hat sich bereits bisher zentral mit Themenbereichen des neuen FB beschäftigt. Wenn bezüglich ihr Zweitmitgliedschaften anzustreben wären, dann zu nahezu allen FBs, was aber nicht sinnvoll erscheint. Da sich der Themenbereich Sicherheit in den letzten Jahren stark erweitert hat, ist zusätzlich geplant, dass im Rahmen des neuen Fachbereichs die FG VIS in mehrere thematisch spezialisiertere Fachgruppen aufgeht.

Die Fachgruppen 3.6.1, 3.6.2 und 2.1.5 haben eine jeweils klar benennbare und in der Vergangenheit etablierte Verankerung in einem Fachbereich. Diese Verankerung soll als Brückenfunktion zum neu zu gründen (Querschnitts-)Fachbereich erhalten bleiben. Die Modalitäten der Doppelmitgliedschaften sollen bilateral mit den betroffenen Fachbereichen geklärt werden.

Die geplante Strukturierung des Fachbereichs ist im Abschnitt 4 detailliert dargestellt.

2 Darstellung der Entwicklung des Fachgebietes

2.1 Entwicklung des Fachgebietes allgemein

Das Fachgebiet IT-Sicherheit hat sich in den vergangenen Jahren aus verschiedenen Disziplinen der Informatik als Querschnittsthema der Angewandten, Praktischen, Theoretischen und Technischen Informatik entwickelt. Die nachfolgenden Aspekte sollen dieser Entwicklung Rechnung tragen sowie die wachsende Bedeutung der Disziplin IT-Sicherheit mit ihrem Leitbildcharakter für die Entwicklung sicherer Informatiksysteme akzentuieren.

Die folgende Aufzählung von Bereichen, deren Gliederung nur vorläufig sein kann, zeigt die Vielfalt der Informatik-Themen im Bereich IT-Sicherheit: technische Grundlagen (u.a. Verlässlichkeit von Informatiksystemen, Zutritts-, Zugriffs- und Zugangskontrolle, Integrität von Daten, Infrastruktursicherheit); organisatorische Grundlagen (u.a. gesetzliche Regelungen, Datenschutz, IT-Sicherheitsmanagement, Sicherheitspolitiken, Sicherheitsevaluationen und Sicherheitszertifizierungen); theoretische Grundlagen (u.a. Sicherheitsmodelle, Kryptographie, Protokollanalysen, Nominale Kalküle, Formale Spezifikation und Verifikation) sowie den Anwendungen und speziellen Techniken (u.a. Elektronisches Geld, Biometrische Authentikations- und Identifikationssysteme, Chipkarten, Firewalls, Intrusion Detection Systeme, Virenscanner).

Wichtige Themen sind darüber hinaus die Dienst- und Systemverfügbarkeit, wobei auch die Verfügbarkeit der Sicherheitseinrichtungen selbst relevant ist. Hierbei sind einerseits technologische Aspekte zu sehen (Zuverlässigkeit, Schutz vor Fehlern, Fehlertolerierende Systeme), aber auch Aspekte der Sicherheit und des Schutzes dieser Systeme, z.B. vor Denial-of-Service Angriffen.

Die nachfolgenden Ausführungen skizzieren kurz die Entwicklung des Fachgebietes in den gesellschaftlichen Bereichen der Hochschulen und Wirtschaft:

- **Wissenschaftliche Entwicklung / Entwicklungen an den Hochschulen**

  Während bislang an den Hochschulen nur Teilaspekte der IT-Sicherheit in Lehrstuhlbeschreibungen und Bezeichnungen Niederschlag fanden (Kryptographie, Kommunikationssicherheit) oder IT-Sicherheit von anderslautenden Bereichen (mit)gelehrt wurde (“Informatik und Gesellschaft”, “Anwendungen der Informatik in Geistes- und Naturwissenschaften”, “Kommunikation in Rechnernetzen”, “Theoretische Informatik”), sind in letzter Zeit an einigen Hochschulen ganze Lehrstühle und Bereiche (Größenordnung C4) für das Gebiet IT-Sicherheit ausgeschrieben worden (Ruhr-Universität Bochum, TU Darmstadt, TU Dresden, Universität Hamburg, TU Hamburg-Harburg, FH Rhein-Sieg, Universität Stuttgart). Hier lässt sich ein deutlicher “Run” auf dieses Thema und eine Konsolidierung der Curricula ausmachen. Die DFG hat 1999 ein Schwerpunktprogramm “Sicherheit in der Informations- und Kommunikationstechnik” eingerichtet.

  Sofern derzeit die wissenschaftliche “Community” noch als überschaubar gelten kann, ist mittelfristig mit einer personellen Vergrößerung, verbunden mit einer stärkeren Ausdifferenzierung und Gruppierung der (fachlichen) Interessen, zu rechnen.

  Trotzdem bleibt die IT-Sicherheit Querschnitts- bzw. Anwendungsthema, wobei einzelne Teilaspekte von anderen Bereichen der Informatik (Verifikation von Hard- und Software, Kommunikation in Netzen), Mathematik (Zahlentheorie, Kryptographie) aber auch Ingenieurdisziplinen (physikalischer Schutz, z.B. Stromversorgung, Brandschutz, Zutrittsschutz) detailliert untersucht und von der IT-Sicherheit genutzt werden.

- **Lehre, Ausbildung und Vernetzung im Bereich IT-Sicherheit**

  In den Gebieten der IT-Sicherheit ist neben der Wissensvermittlung an Hochschulen in den letzten Jahren auch auf dem privaten Sektor eine Verstärkung der Aus- und Weiterbildung zu beo-

bachten, die teilweise durch Zertifizierungsprogramme institutionalisiert und qualitätsgesichert werden. Die an Zahl wachsenden IT-Sicherheitskonferenzen sind teilweise überfüllt.

Außerhalb Deutschlands ist u.a. eine durch die US-amerikanische Regierung angeregte Bildungsinitiative zu benennen, die insbesondere auf dem Gebiet der IT-Security verstärkte Initiativen von Herstellern und angeschlossenen Schulungscentern (in den Bereichen Firewalls, Intrusion Detection Systeme, Policy-based Networking) als auch übergreifender Institutionen verursacht hat (z.B. Aufbau und Vernetzung der CERTs). Der Studiengang Information Security an der Royal Holloway, University of London (http://www.isg.rhul.ac.uk/#MSc) wächst laufend.

Auch in Deutschland bestehen – über das Bundesamt für Sicherheit in der Informationstechnik – koordinierte Initiativen.

- **Wachsende betriebswirtschaftliche Bedeutung der IT-Sicherheit**

  Der Bereich Zuverlässigkeit und Safety hat im wirtschaftlichen Bereich eine lange Tradition, da die Zuverlässigkeit und Verfügbarkeit von Systemen unmittelbar Teil betriebswirtschaftlicher Kalkulationen war (z.B. Nutzungsdauer, Ausfallzeiten). Teilweise wurde die Safety von Systemen auch institutionalisiert (Luftfahrt, Bahn, Straßenverkehr) und einer staatlichen Überwachung unterworfen (u.a. durch Luftfahrt-Bundesamt, Eisenbahn-Bundesamt, Bundesamt für Güterverkehr, aber auch TÜVs, die hoheitliche Aufgaben übernehmen). Eine entsprechende Bedeutung wurde – neben Kostenaspekten – in der Vergangenheit im Bereich der Wirtschaft vereinzelt auch der Zuverlässigkeit der in kritischen Produktionsbereichen eingesetzten IT-Systeme beigemessen.

  Bedingt durch die immer stärkere Vernetzung und die dadurch steigende Abhängigkeit der Produktions- und Verwaltungsprozesse von IT-Systemen besteht in der Wirtschaft wachsender Bedarf an überlebensfähigen IT-Systemen, wozu neben klassischen Zuverlässigkeits- und Safety-Aspekten (Ausfallsicherheit, Funktionssicherheit) mit zunehmender Aufmerksamkeit auch der Schutz vor Angriffen physikalischer oder logischer Natur zu zählen ist.

  Mit stärker werdender Bedeutung von Informationen im betriebswirtschaftlichen Prozess gewinnt neben der Verfügbarkeit auch die Sicherstellung der Authentizität, Integrität, Vertraulichkeit und Nachweisbarkeit von Kommunikation und Unternehmensdaten entscheidende Bedeutung.

- **Wachsende volkswirtschaftliche Bedeutung der IT-Sicherheit**

  Es besteht ein starkes volkswirtschaftliches (und staatliches) Interesse an einer funktionierenden und sicheren Informationsverarbeitung, da durch die wachsende Vernetzung von IT-Systemen auch die Verletzlichkeit zugenommen hat. Sofern nicht durch IT-Sicherheitsprozesse, Schutz- und Notfallmaßnahmen innerhalb der betroffenen Institutionen aufgefangen, können sich sicherheitsverletzende Ereignisse ausbreiten und in ihrer Gesamtheit im Extremfall auch schwere volkswirtschaftliche Folgekosten verursachen. Die gemeinsamen Anstrengungen von Behörden und Unternehmen zur Jahr 2000-Problematik sowie die Folgekosten der Ausbreitung von Emailviren und –würmern sind nur einige Beispiele hierfür.

  Zu nennen sind auch Industrieinitiativen im Bereich der Verfügbarkeit (Raumfahrt, Telekommunikation, E-Commerce). Bei Betrachtung der volkswirtschaftlichen Bedeutung des Electronic Business wird deutlich, dass eine koordinierte Vorgehensweise ganz wesentlich auch zum wirtschaftlichen Erfolg beitragen kann (Bewusstseinsbildung, Ausschreibungen, gesetzliche Anforderungen).

2.2 Entwicklung in der GI

- **Entwicklung des Fachgebiets IT-Sicherheit in der GI**

  Innerhalb der GI wird das Fachgebiet schwerpunktmäßig unter den Sichtweisen “Dependability / Safety” im FA 3.6 (ca. 360 Mitglieder) und in der FG 2.1.5 (ca. 200 Mitglieder) sowie unter der Sichtweise “Kommunikationssicherheit / Security” in der FG 2.0.2 (früher: 2.5.3, ca. 710 Mitglie-

der) behandelt. Weitere Aspekte der IT-Sicherheit finden sich in Fachgruppen weiterer Fachbereiche, u.a. im FB 0 (Formale Grundlagen), FB 5 (E-Business-Szenarien), FB 6 (Rechtliche Aspekte) und FB 8 (Ethische Aspekte). Insgesamt ist das Fachgebiet, gemessen an der im Abschnitt aufgezeigten Breite, als sehr verstreut in der GI anzusehen, wobei die thematisch verwandten Fachgruppen zusammengenommen sowohl von der Mitgliederzahl als auch inhaltlich einen sehr weiten Bereich abdecken.

- **Aktuelle Entwicklung im FB 2**

  Der Fachbereich 2 befindet sich in einer Phase der Neuorientierung, die aufgrund der wachsenden Bedeutung und Vergrößerung einiger der im FB 2 bislang organisierten Gebiete der Informatik auch als natürlich und notwendig anzusehen ist.

  In der Sitzung des Präsidiums im Januar 2001 wurde die (Aus-)Gründung des Bereichs Mensch-Computer-Interaktion als neuer Fachbereich beschlossen, in der Juni-Sitzung 2001 erfolgte eine weitere Aufteilung in die Bereiche Softwaretechnik sowie Datenbanken / Informationssysteme, wobei die bisher im Fachbereich 2 organisierte Fachgruppe 2.0.2 (VIS) organisatorisch derzeit beiden neuen Fachbereichen zugeordnet ist.

- **Neuorientierung des Fachgebiets Sicherheit in der GI**

  Angesichts der derzeit durch die VIS abgedeckten Breite des Gebiets IT-Sicherheit (unter dem Teilaspekt Security) erscheint ein Andocken der FG 2.0.2 an die Bereiche Datenbanken und Softwaretechnik allein thematisch nicht mehr gerechtfertigt. Insbesondere verlangt die starke Anwendungsorientierung der IT-Sicherheit eine Vernetzung mit vielen Bereichen der Informatik, so dass im Zusammenhang mit der Neuorientierung des FB 2 auch die Einordnung des Gebietes IT-Sicherheit zur Debatte stehen sollte. Im Bereich der IT-Sicherheit besteht mittlerweile eine ebenso starke thematische Nähe der FG VIS zu Gebieten wie Zuverlässigkeit (Safety) im Bereich Hard- und Software wie zu Datenbanken, Kommunikation und Softwaretechnik. Für die notwendige Quervernetzung sollte eine bessere Basis gewählt werden, in der das Thema IT-Sicherheit als übergeordnetes Leitthema fungiert.

  Die bislang vorherrschende rein hierarchische Struktur der GI erlaubte nicht die insbesondere im Bereich der IT-Sicherheit notwendige Vernetzung unterschiedlicher Aspekte der Informatik unter dem Blickwinkel der sicheren Informationsverarbeitung.

  Angesichts der nun möglichen strukturellen Quervernetzung (durch mehrfaches Angliedern von Fachgruppen an verschiedene Fachbereiche, durch eine leistungsfähigere Mitgliederverwaltungssoftware) sowie der aus fachlicher Sicht notwendigen Verbreiterung des Gebietes IT-Sicherheit wird innerhalb der GI eine Neuorientierung angestrebt, die in der vorgeschlagenen Form eines neuen Fachbereiches eine breitere Quervernetzung von am Thema interessierten bzw. thematisch im Thema IT-Sicherheit verankerten Fachgruppen gestattet.

3 Zielsetzung des Fachbereichs „Sicherheit – Schutz und Zuverlässigkeit – “

Vision
Aufgaben
Name des Fachbereichs

3.1 Die Vision

Dem Thema ”Sicherheit informatischer Systeme” soll mit der Einrichtung und Ausgestaltung des FB ”Sicherheit – Schutz und Zuverlässigkeit” eine starke Sichtbarkeit innerhalb der GI und auch darüber hinaus verschafft werden. Mit Hilfe eines Fachbereiches zu diesem Thema wollen wir den an dieser Thematik beteiligten Fachgruppen, insbesondere auch den in diesem Gebiet arbeitenden Informatikern, ein Forum bieten, in dem sie ihr Fachthema, organisiert in Fachgruppen, wiederfinden. Neben der rein wissenschaftlichen Arbeit soll der Fachbereich einen fachlichen Austausch zwischen Wissenschaft und Praxis ermöglichen.

Sicherheit ist ein Querschnittsthema. Für den Fachbereich wird daher eine hohe Flexibilität hinsichtlich der Möglichkeiten zur Quervernetzung verschiedener Gruppen und Themen in der GI gefordert. Das betrifft auch die Einbindung neuer, ggf. bislang auch “fachfremder” Themen, für die auch neue Fachgruppen entstehen oder auch hier übergreifende Kooperationen mit anderen Fachgesellschaften[1] entstehen können. Diese Quervernetzung sollte sowohl in gemeinsamen Veranstaltungen zum Ausdruck kommen, aber auch in der starken Berücksichtigung anderer Themen aus Informatik und anderen Bereichen bei der Diskussion von IT-Sicherheit. Sicherheit ist kein Selbstzweck, sondern wichtig zur Erfüllung gesellschaftlicher, technischer oder organisatorischer Bedürfnisse.

Die GI könnte mit einem Fachbereich zum Thema Sicherheit ein verständliches und sichtbares Thema vorweisen, Kompetenz zeigen und sich deutlich positionieren. Neben der Veröffentlichung von Stellungnahmen, die bereits jetzt vom Präsidiumsarbeitskreis “Datenschutz und IT-Sicherheit” erarbeitet werden, gehört dazu auch der “Community”-Aspekt. Die GI soll in diesem Thema nicht nur auch etwas zu sagen haben, sondern sie soll DER Träger der “Community” im Bereich der IT-Sicherheit sein.

Es muss Ziel der GI sein, dass in ihr alle im Zusammenhang mit informatischen Systemen stehenden sicherheits- und verfügbarkeitsrelevanten Themen im deutschsprachigen Raum konzentriert werden und die GI als Anlaufstelle für Praxis und Theorie auftritt. Gerade die GI könnte hier als neutrale Instanz fungieren im Hinblick auf Bewusstseinsbildung, Definition von Anforderungen, Einordnung technischer Entwicklungen.

Es wird erwartet und gewollt, dass sich bestehende und auch neu zu gründende Fachgruppen zu verschiedenen sicherheitsrelevanten Themen dem FB Sicherheit angliedern. Die GI bietet den neu entstehenden Hochschul-Fachbereichen, Lehrstühlen und dem Mittelbau eine wissenschaftliche Community-Heimat für ihr Fachgebiet an.

Gleichzeitig entsteht eine Vernetzung zwischen Wissenschaft und Praxis im Themenbereich IT-Sicherheit. Die GI wird für Fachleute auf diesem Gebiet fachlich interessant, wenn diese den Aufbau von Know-How auf den Gebieten der Safety und Security institutionalisiert.

Die Initiatoren sind davon überzeugt, dass dieses Thema langfristig eine starke Relevanz und Anziehungskraft ausüben wird. Wir gehen davon aus, dass fast alle GI-Mitglieder mittelbar oder unmittelbar von dem Thema betroffen sind und als Zielgruppe für den Fachbereich wenigstens 25 % der Mitglieder in Frage kommen.

---

[1] Das müssen nicht nur Fachgruppen von ITG/VDE und VDI sein.

3.2 Aufgaben des neuen Fachbereichs

Die Aufgaben des neuen Fachbereichs lassen sich mit den folgenden Schlagworten umreißen, jedoch nicht vollständig erfassen. Sie sind sozusagen als Mindestaufgaben zu sehen.

Unterstützung der wissenschaftlichen Arbeit auf den Gebieten der IT-Sicherheit

- Überblick über Schwerpunkte der verschiedenen Hochschul-Fachbereiche zum Thema Sicherheit
- Fach- und Arbeitsgruppen zu verschiedenen Themen
- wissenschaftliche Tagungen (VIS, ...)
- wissenschaftliches Journal (evtl. Kooperation mit der DuD, ...)
- wissenschaftliche Definitionen zu den Themen der Sicherheit informatischer Systeme

Vernetzung Wissenschaft, Industrie und Gesellschaft

- Tagungen und Veranstaltungen, auf denen wissenschaftliche und Praxisthemen verknüpft werden
- Seminare (z.B. in Zusammenarbeit mit der DIA)
- Webbasierte Plattform
- Moderation von Themen rund um die Sicherheit informatischer Systeme
- Quervernetzung mit ITG und VDI-Gruppen, z.B. auch mit Fachgruppen der OCG oder SIS
- Management von Sicherheit, Umsetzung
- schnellerer Transfer von wissenschaftlichen Arbeiten in die Praxis
- Kooperation mit dem BSI und den Datenschutzbeauftragten des Bundes und der Länder

Vernetzung mit den Hochschulen

- Die Inhaber sowie Mitarbeiter von Lehrstühlen zum Thema Sicherheit müssen in der Sicherheits-Community der GI organisiert sein. Die GI bietet im Gegenzug mit dem FB eine Basis dafür an.
- Hineinziehen von Studierenden vor dem Diplom in die Community
  - Studierendenprogramme
  - Förderung des Austauschs zwischen Wissenschaft und Praxis
- Erreichen von Promotionsstudierenden
  - wissenschaftliche Arbeitsgruppen
  - kleine Community, aber Gelegenheit für notwendige Publikationen
- Präsenz in den Lehrveranstaltungen
  - wenn Materialien in Pro- und Seminaren sowie Zitate in Studien- und Diplomarbeiten auch auf Publikationen der GI verweisen, besteht die Notwendigkeit (= Chance), dass sich die Studierenden, Promotionsstudierende und Lehrverpflichteten damit sichtbar auseinandersetzen.

3.3 Name des neuen Fachbereichs

Die Namensfindung des neuen Fachbereichs hat bislang viel Zeit in Anspruch genommen und musste mit einem hohen Maß an Sensibilität vorgenommen werden, da aufgrund der in der Vergangenheit vollzogenen organisatorischen unterschiedlichen Entwicklung von Teilbereichen der Sicherheit sich auch Begrifflichkeiten unterschiedlich entwickelt haben. Nach intensiver Diskussion schlagen die Initiatoren gemeinsam als Namen für den Fachbereich vor:

Sicherheit

mit dem Untertitel: **Schutz und Zuverlässigkeit**

Namenszusätze wie “IT-”, “IV-”,”der Informatik”, “der Informationstechnik” oder “der Informationsverarbeitung” wurden letztlich mehrheitlich abgelehnt, da davon ausgegangen wird, dass durch die Markierung als Fachbereich der Gesellschaft für Informatik der informatische Kontext ausreichend dargestellt wird.

4 Struktur des neuen Fachbereichs

4.1 Aufbauorganisation

Der in diesem Abschnitt dargestellte Aufbau des Fachbereichs entspricht dem derzeitigen Diskussionsstand. Der Fachbereich wird bei Einsetzung durch das Präsidium der Gesellschaft für Informatik aus den initiierenden Fachgruppen

- Verlässliche IT-Systeme (bisher 2.0.2/2.5.3)
- Fehlertolerierende Rechensysteme (FG 3.6.1)
- ENCRESS (FG 3.6.2)
- ADA (FG 2.1.5) und

gebildet, wobei die bisherige Fachgruppe „Verlässliche IT-Systeme" komplett in den neuen FB wechselt, während die weiteren drei Fachgruppen durch Doppelmitgliedschaft in zwei Fachbereichen beteiligt sein wollen.

Es ist jedoch wichtig, darzustellen, dass diese Struktur so nur zu Beginn bestehen soll. Es ist beabsichtigt, alsbald nach Gründung des Fachbereichs eine Neusortierung der Fachthemen und –gruppen vorzunehmen. Formell (gemäß GOGL) muss dies jedoch nach Einsetzung des FB durch dessen Leitungsgremium erfolgen, insofern kann an dieser Stelle nur der geplante Aufbau dargestellt werden.

Im Vorfeld der Gründung des Fachbereichs wurden hierzu verschiedene Gestaltungsmodelle diskutiert. Prinzipiell soll jedoch Interessierten ein möglichst großer Entfaltungsspielraum bei der Positionierung ihrer Fachthemen im Gebiet Sicherheit gegeben werden. Das ist durch das Leitungsgremium zu organisieren.

FB-Leitungsgremium

Das FB-Leitungsgremium wird vom Präsidium vorläufig eingesetzt und nach einer Übergangsfrist durch ein gemäß Wahlordnung gewähltes Leitungsgremium ersetzt werden. Das Verfahren für die Bildung eines vorläufigen Leitungsgremiums sowie Vorschläge für dessen Besetzung sind im Vorfeld ausführlich diskutiert worden.

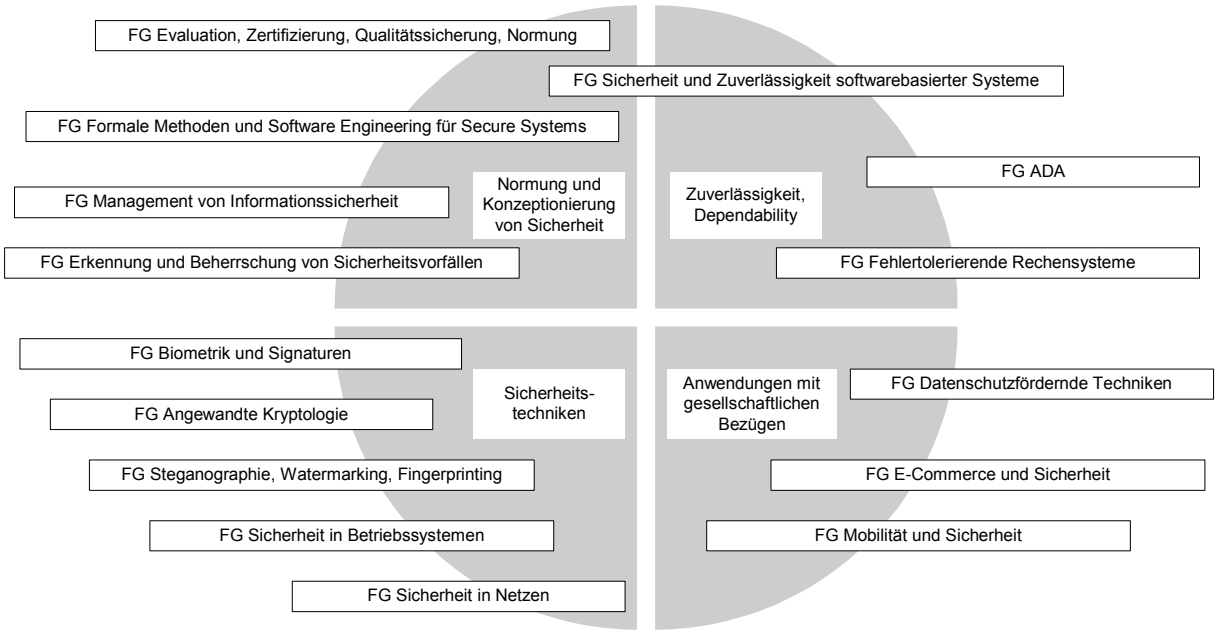
Üblicherweise wird nach einer Startfrist von 3 Jahren das Leitungsgremium "indirekt" gebildet, u.a. aus den Sprechern der Fachgruppen des Fachbereichs. Diese gewöhnliche und gemäß GOGL implizierte Vorgehensweise soll auch hier angewendet werden.

Die Besetzung des Leitungsgremiums wurde unter den Initiatoren abgestimmt und erfolgt sowohl unter dem Kriterium der Arbeitsfähigkeit des Gremiums als auch unter einer möglichst repräsentativen und ausgewogenen Berücksichtigung der einzelnen Interessensgruppen unter den Initiatoren.

Die Benennung zweier Stellvertreter erfolgt unter dem Gesichtspunkt einer Zuarbeit zum Sprecher sowohl von formaler (FB-Organisation, finanzielle Fragen, etc.) als auch thematischer Seite (inhaltliche Koordination, Öffentlichkeitsarbeit, thematische Entwicklung des FB). Zusätzlich wurde berücksichtigt, dass die in der Startphase anfallende Arbeitslast (sowohl beim Aufbau des FB als auch seiner evtl. neuen Untergliederungen) möglichst breit verteilt wird.

Fachgruppen

Derzeit ist geplant, nach Einsetzung des Fachbereichs bis zu 16 Fachgruppen zu etablieren (s. Abbildung):



Folgende Besonderheiten sollen hierbei berücksichtigt werden:

- Insbesondere Fachgruppen aus Bereichen der “Dependability” sollten neben einer thematischen Vernetzung im Bereich der Sicherheit auch in ihrem “Basis”-Fachgebiet in den Fachbereichen 2 bzw. 3 eingebunden sein. Organisatorisch soll dies über eine Doppelmitgliedschaft gewährleistet werden.
- Die Fachgruppen sollen in Übereinstimmung mit den aktuellen Entwicklungen in der GI (Andocken von Fachgruppen, Vernetzung, Mitgliederverwaltungssoftware) nicht durchnumeriert, sondern mit aussagekräftigen Namen oder Kurzbezeichnungen versehen werden.

Arbeitskreise für übergeordnete Themen des Fachbereichs

- FB-Entwicklung
- Safety/Security-Webserver
- FB-Publikationen

Mitgliederzahl

Sofern die Mitgliederzahl lt. GI-Datensammlung 6/2001 zugrunde gelegt wird, so kann zu Beginn von ca. 1200 Mitgliedern ausgegangen werden, die durch die initiierenden Fachgruppen in den Fachbereich eingebracht werden.

Da mit Gründung des Fachbereichs die Sichtbarkeit des Themas Sicherheit verstärkt wird, wird davon ausgegangen, dass sich viele weitere Mitglieder, die dieses Thema betrifft, dem Fachbereich bzw. den untergliederten Fachgruppen zuordnen werden.

Umworben werden dabei nicht nur bestehende GI-Mitglieder, sondern es sollen auch potentielle Neumitglieder für die GI hinzugewonnen werden.

Finanzierung

Die Finanzierung des Fachbereiches richtet sich nach den allgemeinen Richtlinien der GI.

Der Fachbereich muss, wie andere auch, seine Ausgaben durch eigene Einnahmen – ergänzt um ein FB-Budget seitens "der GI" – bestreiten. Der Fachbereich muss eigene Einnahmen durch Mitgliedsbeiträge, Veranstaltungserlöse und dergleichen erwirtschaften.

Für die Gründung wird jedenfalls beantragt, den Fachbereich gleichberechtigt mit anderen Fachbereichen zu behandeln, womit intendiert ist, dass der Fachbereich – wie alle anderen auch – von der GI einen jährlichen Verfügungsrahmen (Budget) zur Verfügung gestellt bekommt, aus dem die mindestens anfallenden und von der GI geforderten Aufwände (Kosten für Briefwahlen, Rundsendungen, FB-Verwaltung, ggf. Vorfinanzierungen) gedeckt werden können. Zeitschriften, Tagungen, etc. müssen aber aus eigenen Einnahmen des FB erwirtschaftet werden.

4.2 Vorstellung der Fachgruppen und Arbeitskreise

In den folgenden Abschnitten werden die Arbeitsgebiete der Fachgruppen vorgestellt. Zusätzlich werden einige Arbeitskreise vorgestellt, die übergeordneten Charakter haben sollen und daher direkt dem Fachbereich zugeordnet werden.

FG Management von Informationssicherheit

Initiatoren:

- Helmut G. Stiegler helmut.stiegler@sti-consulting.de
- Peer Reymann pr@itqs.de
- Isabel Münch muench@bsi.de
- Wolfgang Behnsen wolfgang.behnsen@t-systems.de
- Jens Nedon nedon@consecur.de
- Andreas Prass andreas.prass@si-bw.de
- Frank F. Damm Frank.F.Damm@bku.db.de

Kurzbeschreibung:

Informationssicherheit kann nicht allein durch den Betrieb technischer Sicherheitskomponenten erreicht werden, denn diese entfalten erst ihre Wirkung, wenn ihr Einsatz sich an den tatsächlichen Sicherheitsbedürfnissen der jeweiligen Organisation orientiert und wenn dies auch in den organisationsinternen Abläufen verankert ist.

Durch Sicherheitsmanagement soll eine organisationsweite Koordination und Bündelung aller Aktivitäten in der Informationssicherheit erreicht werden. Neben der Definition des Sicherheitszieles und der Ermittlung der dafür notwendigen Maßnahmen ist dafür die erfolgreiche Etablierung von Sicherheitsprozessen in der jeweiligen Organisation. Sicherheitsmanagement ist daher die notwendige Schnittstelle zwischen informationstechnischen Schutzmaßnahmen und dem Risikomanagement einer Organisation. Es bildet damit zugleich eine Brücke zwischen informatischen und betriebswirtschaftlichen Sichtweisen des Sicherheitsbegriffs.

Die dabei zu bewältigenden Aufgaben sind heute Gegenstand von Firmen, Öffentlichen Verwaltungen, Normungsgremien sowie öffentlichen und privaten Zertifizierungsstellen, wobei oft nur Teilaspekte behandelt werden.

Schwerpunkt der FG ist, die verschiedenen Ansätze systematisch zu bündeln, wobei bekannte sicherheitstechnische Ansätze integriert werden sollen. Die Themengebiete lassen sich wie folgt umreißen:

- Leitbilder der Informationssicherheit

- Sicherheitsleitlinien und –normen in Organisationen (Policies)
- Rahmenbedingungen für Informationssicherheit
  - gesetzliche (Datenschutz, Mitbestimmung, Zulässigkeit von Schutzmaßnahmen)
  - rechliche (vertragliche Regelungen, Haftung, etc.)
  - soziokulturelle (Freiheit vs. Kontrolle, psychologische Aspekte der Sicherheit)
- Etablierung von Informationssicherheit in Organisationsstrukturen
  - Sicherheitsprozesse, -Workflows
  - Sicherheit im laufenden Betrieb
  - Return on Investment
  - Schaffung einer Sicherheitskultur in der Organisation
- Risiken
  - Analyse und Bewertung von Risiken
  - technisches und betriebswirtschaftliches Risikomanagement
  - Umgang mit Restrisiken, Vorfall-Management und “lernende Organisation”
- Auswahl und Umsetzung von Sicherheitsmaßnahmen
  - Etablierung von “Sicherheitsmanagementsystemen”
  - Zusammenspiel von organisatorischen, personellen, baulichen und technischen Maßnahmen
- Schulung, Sensibilisierung und Motivation für Informationssicherheit
- Qualitätssicherung und Revision von Informationssicherheit
  - Auditierung und Zertifizierung, u.a. Vergleichbarkeit von Zertifikaten
  - Rolle und Einsatz evaluierter IT-Produkte
  - Self-Assessments, Checklisten und Assessment-Tools

Die Fachgruppe greift dabei gezielt auch Ergebnisse anderer Fachgruppen auf, um zu untersuchen, wie die dort behandelten Aspekte organisatorisch gebündelt und in Organisationen eingesetzt werden können.

FG Erkennung und Beherrschung von Sicherheitsvorfällen

Initiatoren:

- Klaus-Peter Kossakowski kpk@pre-secure.de
- Ulrich Flegel flegel@ls6.informatik.uni-dortmund.de
- Klaus Brunnstein brunnstein@informatik.uni-hamburg.de
- Arslan Brömme arslan@aviomatik.de
- Michael Meier mm@informatik.tu-cottbus.de
- Jens Nedon nedon@consecur.de
- Andreas Prass andreas.prass@si-bw.de
- Markus Nolte nolte@mlrp.de

Kurzbeschreibung:

Planung und Einsatz von Schutzmaßnahmen erfolgen mit dem Ziel einer Minimierung des verbleibenden Risikos für die Organisation. Dieses sogenannte Restrisiko entsteht dadurch, dass

- auch Schutzmaßnahmen überwunden oder umgangen werden können,
- auch Fehler bei der Auswahl und dem Einsatz von Schutzmaßnahmen geschehen,
- die Notwendigkeit von Schutzmaßnahmen gar nicht erkannt wird und damit auch keine Maßnahmen eingesetzt werden,
- Risiken auch durch Abwälzung z.B. auf Versicherungen abgedeckt und verringert werden können, allerdings dabei nicht alle Auswirkungen und Folgeschäden bedacht wurden,
- Risiken aus betriebswirtschaftlichem Kalkül teilweise bewusst in Kauf genommen werden (müssen).

Hierbei wird oft übersehen, dass Restrisiken ein teilweise sehr hohes Schadenpotential beinhalten können und nur aufgrund einer sehr geringen Eintrittshäufigkeit als beherrschbar erscheinen. Eine Organisation muss sich gerade angesichts dieser Betrachtungsweise jedoch darauf einstellen, dass Ereignisse mit sehr hohem Schadenpotential trotzdem eintreten können, wobei die bestehenden Schutzmaßnahmen nicht wirken, da die Risiken billigend in Kauf genommen wurden.

Die Erkennung und Beherrschung solcher Situationen ist Fokus dieser Fachgruppe, wobei der Schwerpunkt auf informationstechnische Fragestellungen gerichtet sein soll.

Die Themen der Fachgruppe lassen sich im einzelnen wie folgt charakterisieren:

- Erkennung und Meldung von Sicherheitsvorfällen,
  z.B. technischen, logischen und Informationsangriffen,
  z.B. durch Intrusion Detection Systeme und andere Meldewege, auch aus dem Objektschutz
- Eindämmung von Schadensfällen
- Wirkungsanalyse von Vorsorgemaßnahmen zur verbesserten Erkennung und Eindämmung von Schäden
- Untersuchung und Bewertung von Sicherheitsvorfällen,
  Vorgehensweisen und Techniken für eine juristisch verwertbare Beweiserhebung und –sicherung, Rückverfolgung von Angriffen und Urhebern
- Aufrechterhaltung bzw. Wiederherstellung eines sicheren IT-Betriebs nach Sicherheitsvorfällen, Business Continuity (Disaster Recovery, Survivability) bei Krisen und bei tagtäglichen Angriffen
- Notfallorganisation und Krisenmanagement,
  Organisation von Computer-Notfallteams (CERTs, Computer Emergency Response Teams) und Krisen-Managementteams
- Strategien für eine überlebensfähige IT-Organisation und die Beherrschbarkeit schwerwiegender Schadensfälle
- Auswirkungen von Sicherheitsvorfällen – und der Reaktion auf solche – auf andere Bereiche, insbesondere den Schutz kritischer Infrastrukturen und die gesellschaftliche Akzeptanz der risikobehafteten IT

Insbesondere für die Diskussion organisatorischer und rechtlicher Fragestellungen, z.B. die Notfallorganisation, den Schutz kritischer Infrastrukturen oder die Vorgehensweisen für eine juristisch verwertbare Beweissicherung bei Vorfällen, wird eine enge Zusammenarbeit mit anderen Fachgruppen gesucht.

FG Formale Methoden und Software Engineering für Secure Systems

Initiatoren:

- Jan Jürjens juerjens@in.tum.de
- David Basin basin@informatik.uni-freiburg.de
- Maritta Heisel heisel@wotan.cs.uni-magdeburg.de

- Dieter Hutter hutter@dfki.de
- Heiko Mantel mantel@dfki.de
- Thomas Santen santen@cs.tu-berlin.de
- Guido Wimmel wimmel@in.tum.de
- Burkhart Wolff wolff@informatik.uni-freiburg.de
- Thilo Zieschang thilo.zieschang@eurosec.com
- Andreas Pfitzmann pfitza@inf.tu-dresden.de

Kurzbeschreibung:

Zielsetzung dieser Arbeitsgruppe ist es, im Bereich Computer- und Informationssicherheit (im Sinne von Security) ein Diskussionsforum im deutschsprachigen Raum zu bieten, das sich mit der Grundlagenforschung und Anwendung formaler oder mathematisch präziser Techniken im Software-Engineering beschäftigt.

Die Entwicklung von Systemen, die Security Anforderungen genügen müssen, beinhaltet Herausforderungen, die ueber die Problematik von Sicherheit im Sinne von Safety hinausgehen. Nicht zufälliges Fehlverhalten, sondern mutwillige Angriffe stehen im Vordergrund, die spezielle Techniken (etwa den Einsatz von Kryptographie) erfordern, und die Neubewertung traditioneller Techniken im Bereich Safety (etwa Markovmodellierung) in Bereich Security erfordern.

Es werden viele Systeme entworfen und realisiert, in denen im Nachhinein schwere Sicherheitslücken in Entwurf und Implementierung gefunden werden, die zum Teil schlagzeilenträchtige Angriffe ermöglichen. Das liegt einerseits daran, dass mathematisch präzise Definitionen für so grundlegende Begriffe wie „Security" oder „secure system" fehlen oder sich nicht unmittelbar auf einen Entwicklungskontext abbilden lassen. Zum anderen unterstützen etablierte Methoden des Software-Engineering die Berücksichtigung von Sicherheitsaspekten noch unzureichend.

Es ist also notwendig, die Diskussion über Grundbegriffe weiterzutreiben und diese auf Notationen und Prozesse abzubilden, die die ingenieurmäßige Entwicklung sicherheitskritischer Systeme effizient unterstützen.

Themenbereiche für die FG innerhalb des Fachbereichs Sicherheit sind demnach:

- die mathematisch / logisch fundierte Definition von Sicherheits-Grundbegriffen
- Anpassung von Techniken aus dem Bereich Safety auf die spezielle Situation im Bereich Security (etwa das Erarbeiten quantifizierbarer Kenngrößen von Sicherheit)
- die Modellierung und Spezifikation von Sicherheitsanforderungen, insbesondere mit formalen Techniken,
- die formale Spezifikation sicherheitskritischer Teile eines Systems,
- der Entwurf, die Dekomposition und die Komposition von softwarebasierten Systemen unter systematischer und nachweisbarer Realisierung von Sicherheitseigenschaften
- die Abbildung (Verfeinerung) von Sicherheitseigenschaften auf real-existierende Sicherheitstechnologien sowie die Untersuchung der methodischen Probleme solcher Verfeinerungen
- die Entwicklung von Verifikationstechniken und -methoden zum Nachweis sicherheitsrelevanter Eigenschaften von Spezifikationen oder Programmen, auch mit Unterstützung etwa durch Werkzeuge wie Modelchecker, Theorembeweiser oder CASE-tools
- die Untersuchung der Leistungsfähigkeit von Testverfahren auf Basis formaler Modelle zur Demonstration von Sicherheitseigenschaften, insbesondere die Generierung von Testsequenzen aus einer Spezifikation zur Überprüfung sicherheitsrelevanter Eigenschaften einer Implementierung
- die Integrierung von Sicherheitsaspekten in den Entwicklungsablauf in der Praxis, unter Verwendung und Anpassung industriell gebräuchlicher Entwurfsmethoden, Notationen und Prozesse.

Besonders wichtig ist die Erkenntnis, dass Security eine ganzheitliche Eigenschaft von Systemen ist. Die Diskussion innerhalb der Arbeitsgruppe soll deshalb insbesondere den Austausch zwischen Experten verschiedner fachlicher Ausrichtung fördern und zu einem umfassenden Verständnis der Problematik beitragen.

FG Sicherheit in Betriebssystemen

Initiatoren:

- Amon Ott ott@compuniverse.de
- Christian Stüble stueble@cs.uni-sb.de
- Arnd Weber Arnd.Weber@itas.fzk.de

Kurzbeschreibung:

Die Fachgruppe befasst sich mit allen Sicherheitsaspekten innerhalb von Betriebssystemen. Schwerpunkte sind:

- Modelle zur Zugriffskontrolle
- Lokale Authentisierungsverfahren (Schnittstelle zur Biometrik etc.)
- Sicherheit als bestimmendes Designmerkmal
- Konkrete Sicherheitsmerkmale und -lücken bestehender Systeme
- Sicherheitserweiterungen bestehender Systeme, speziell aus dem Open-Source-Bereich

Eine übergreifende Zusammenarbeit mit einer Fachgruppe “Sicherheit in Netzen” wäre wünschenswert, insbesondere mit Schwerpunkten “Verteilte Systeme” und “Authentisierung”.

FG Sicherheit in Netzen

Initiatoren:

- Matthias Jänichen mj@percomp.de
- Kai Rannenberg kair@microsoft.com
- Dogan Kesdogan kesdogan@informatik.rwth-aachen.de
- Frank F. Damm Frank.F.Damm@bku.db.de
- Andreas Prass andreas.prass@si-bw.de
- Rüdiger Grimm ruediger.grimm@tu-ilmenau.de

Kurzbeschreibung:

Die Fachgruppe beschäftigt sich mit Gefahren und deren Abwehr, die durch die zunehmende Vernetzung von ITK-Systemen entstehen.

Auf der einen Seite sollen Gefahren betrachtet werden, die durch die technische Vernetzung an sich entstehen. Die Vernetzung unterschiedlicher Systeme kann Regelkreise aktivieren oder Rückkopplungen auslösen. Diese müssen schon im Vorwege erkannt und verhindert werden.

Auf der anderen Seite hat die Vernetzung von Systemen ein erhebliches Missbrauchspotenzial. Die jüngsten zerstörerischen Angriffe von Hackern oder Virenautoren sind allgemein aus den Medien bekannt. Weniger offensichtlich sind die schon heute genutzten Möglichkeiten, die Netze kriminell oder zur Überwachung zu missbrauchen. Die Betreiber eines Systems benötigen Verfahren, Werkzeuge und Know-how um sich zu schützen.

Die Fachgruppe fördert die Entwicklung solcher Verfahren und Werkzeuge, die sowohl existierende Netze entschärfen und bei der Entwicklung neuer Vernetzungen greifen.

Für die AGs innerhalb dieser FG bietet es sich an, das ISO/OSI-Schichtenmodell zu adaptieren und entsprechend aufzubauen:

1-4: Sichere (fehlerfreie) Kommunikation zwischen Systemen, sichere Netzprotokolle,

5-7: Content-Security, Anti-Virus Techniken (Überwachung und Filterung von systemgefährdenden Inhalten - Viren, Würmer, Trojaner)

FG Biometrik und Signaturen

Initiatoren:

- Arslan Brömme broemme@informatik.uni-hamburg.de
- Petra Wohlmacher petra.wohlmacher@regtp.de
- Willem Froehling speaker@koram.de
- Thomas Gast thomas.gast@bsi.bund.de
- Olaf Gellert gellert@pca.dfn.de
- Martin Johns m.johns@web.de
- Oliver Kasch olli@kasch-hamburg.de
- David Ochel david@atsec.de
- Caroline Mojert cm@enisrat.net
- Astrid Mayerhöfer astrid.mayerhoefer@ipsi.fraunhofer.de
- Kathrin Schier kathrin.schier@eurokartensysteme.de
- Till Teichmann till.teichmann@hypovereinsbank.de

Kurzbeschreibung:

Die Fachgruppe Biometrik und Signaturen widmet sich thematisch den Grundlagen, Methoden, Techniken, Abläufen und Realisierungen zur Sicherung der Authentizität und Integrität beteiligter Entitäten beim Einsatz von Informations- und Kommunikationssystemen für Anwendungen mit Sicherheitsbedarf sowie deren organisatorischen und rechtlichen Rahmenbedingungen. Hierbei werden konstruktive Vorgehensweisen und Bedrohungsanalysen behandelt.

Die Fachgruppe versteht sich als fachliches Diskussionsforum für Wissenschaftler, Entwickler, Anwender und Vertreter von Aufsichtsstellen und Regulierungsbehörden im deutschsprachigen Raum für dieses Forschungs- und Anwendungsgebiet.

Die Zugehörigkeit der Fachgruppe Biometrik und Signaturen zum GI-Fachbereich „Sicherheit“ ergibt sich aufgrund des Verständnisses von Authentizität und Integrität als grundlegende Sicherheitseigenschaften, die für eine Vielzahl sicherheitserfordernder Anwendungen etwa im Umfeld von e-Commerce, e-Business, e-Government und e-Democracy vorausgesetzt werden und diese erst ermöglichen.

Zur Sicherung der Authentizität von Entitäten und der Authentizität/Integrität von Daten und Prozessen werden unterschiedliche Methoden diskutiert. Die Methoden für die Sicherung der Authentizität von Entitäten basieren hauptsächlich auf Wissen (Passwörter, Passphrasen, PINs, TANs), Besitz (Smart-Cards, Security-Tokens), Eigenschaft (Biometrische Merkmale), Lokation, Zeit und deren Kombinationen. Die Sicherung der Authentizität/Integrität von Daten und Prozessen basiert hauptsächlich auf elektronischen Signaturverfahren, die in Verbindung mit unterschiedlichen anwendungsabhängigen Zertifikaten zum Einsatz kommen. Rechtliche und organisatorische Rahmenbedingungen umfassen den Datenschutz im engeren und Privacy im weiteren Sinne sowie Zertifizierungsinfrastrukturen, mit denen öffentliche Schlüssel authentisch bereitgestellt werden können, und Biometrischen Infrastrukturen, mit denen biometrische Merkmale von Personen verifiziert bzw. identifiziert werden können.

Zwei Themengebiete mit herausragender Bedeutung für die Authentizitäts- und Integritätssicherung von Anwendungen für die e-Economy und e-Society sind die Biometrik und die Signaturen:

Die Biometrik beschäftigt sich mit der Vermessung und der Auswertung biometrischer Merkmale von Personen (statisch- und dynamisch-physiologische sowie Verhaltenscharakteristika) für Anwendungen in den Bereichen der Zugriffs- und Zugangskontrolle sowie Personenidentifikation, -analyse und -verfolgung in

lokalen und vernetzten Systemen. Die Betrachtungen der Fachgruppe im Umfeld der Biometrik beziehen sich hierbei auf die nachstehenden Aspekte, ohne durch diese begrenzt zu sein:

- Biometrische Algorithmen, Signaturen und Datenbanken
  Auswertung biometrischer Merkmale mit adäquaten Algorithmen zur Berechnung biometrischer Signaturen sowie der Gestaltbarkeit von biometrischen Datenbanken in Systemen.
- Biometrische Techniken
  Verfahren zur Erfassung biometrischer Merkmale unter Berücksichtigung von Safety- und Security-Aspekten.
- Zugriffs- und Zugangskontrolle mittels biometrischer Systeme
  Biometrische Authentikation (im weiteren Sinne) sowie Biometrische Verifikation und Identifikation (im engeren Sinne) im Rahmen von mandatorischen, diskretionären und rollenbasierenden Zugriffskonzepten
- Test und Bewertung biometrischer Algorithmen und Systeme
  Testverfahren, -konzepte und -ergebnisse mit und ohne Berücksichtigung der Anwendungsumgebung.
- Angreifbarkeit biometrischer Algorithmen, Techniken und Systeme
  Beurteilung der Stärken und Schwächen biometrischer Verfahren durch Diskussion von Bedrohungsanalysen, Fälschbarkeit biometrischer Merkmale, Täuschbarkeit biometrischer Systeme
- Überwachung und Fahndung mit Biometrik
  Personenidentifikation und -verfolgung, Verhaltensanalyse, Ausweise, Biometrische Merkmalsspuren für die Fahndung, Biometrische Systeme für die Terrorbekämpfung
- Aspekte des Datenschutzes beim Einsatz biometrischer Methoden
  Biometrische Daten und informationelles Selbstbestimmungsrecht, Gestaltbarkeit biometrischer Systeme unter Berücksichtigung von Datenschutz und Privacy

Signaturen werden eingesetzt zur Sicherung der Authentizität und Integrität von Daten sowie zur Sicherung der Authentizität von Entitäten auf der Basis zugrunde liegender kryptographischer Mechanismen. In entsprechende technische, organisatorische und rechtliche Rahmenbedingungen in Form von Zertifizierungsinfrastrukturen eingebettet ermöglichen Signaturen die Realisierung einer definierten Verbindlichkeit der über öffentliche oder private Netze übertragenen Informationen aber auch der in Archivierungssystemen bereitgestellten Daten. Die Betrachtungen der Fachgruppe im Umfeld der Signaturen beziehen sich hierbei auf die nachstehenden Aspekte, ohne durch diese begrenzt zu sein:

- Kryptographische Algorithmen für Signaturverfahren
  Nutzung, Implementierung und Adaptierung von Signaturverfahren auf Basis kryptographischer Grundlagen
- Sicherheitsdienste und -mechanismen basierend auf Signaturen
  Sicherung der Authentizität von Entitäten, Authentizität und Integrität von Daten, Nichtabstreitbarkeit
- Produkte und Systeme für den praktischen Einsatz von Signaturen
  Bewertung unterschiedlicher Signaturklassen, Security-Tokens, Testverfahren, -konzepte und -ergebnisse mit und ohne Berücksichtigung der Anwendungsumgebung
- Integration von Signaturen in organisatorische, technische & rechtliche Rahmenbedingungen
  Zertifizierungsinfrastrukturen für öffentliche Schlüssel (Public-Key-Infrastrukturen – PKIs) zur Schaffung von Verbindlichkeit, Schaffung von Vertrauen in Signaturanwendungen
- Anwendungen unter Nutzung von Zertifizierungsinfrastrukturen
  Gestaltung von Anwendungsumgebungen, Einsatzbereiche im e-Commerce und e-Government
- Aspekte rechtlicher Rahmenbedingungen
  EU-Richtlinie zur elektronischen Signatur, Signaturgesetze & Signaturverordnungen, Datenschutz

- Standardisierung und Interoperabilität
  Kryptographische Mechanismen, infrastrukturbedingte Protokolle, Anwendungen, Signaturgesetz-Konformität, CC- und ITSEC-Schutzprofile und -Evaluierungen

Die Fachgruppe Biometrik und Signaturen strebt eigene Workshops und Veranstaltungen sowie Tagungen im Verbund mit den anderen Fachgruppen des FB „Sicherheit“ an, um den fachlichen Austausch im Rahmen der GI zu ermöglichen.

FG Angewandte Kryptologie

Initiatoren:

- Patrick Horster	patrick.horster@uni-klu.ac.at
- Thilo Zieschang	thilo.zieschang@eurosec.com
- Martin Welsch	
- Helmuth Reimer	teletrust@t-online.de
- Norbert Pohlmann	norbert.pohlmann@utimaco.de
- Peter Kraaibeek	peter@kraaibeek.com
- Gerhard Weck	GerhardWeck@compuserve.com
- Stephan Teiwes	
- Christian Kolmitzer	

Kurzbeschreibung:

In der Fachgruppe werden alle Aspekte der modernen (symmetrischen und asymmetrischen) Kryptologie, der kryptologischen Protokolle und deren jeweiliger Bezug zu gegenwärtigen und zukünftigen Anwendungen behandelt. Insbesondere stehen Aspekte der angewandten Kryptologie im Vordergrund, ohne dabei die Grundlagenforschung zu vernachlässigen. Zudem werden die relevanten Entwicklungen in den Bereichen DNA- und Quanten-Computer berücksichtigt. Die Fachgruppe soll ausschließlich fachbezogen arbeiten, in Fragen der Kryptopolitik sind alle Standpunkte zu berücksichtigen. Die Fachgruppe fördert den Einsatz kryptographischer Techniken für alle relevanten Anwendungen.

Neben Verfahren der angewandten Kryptologie sollen auch solche Aspekte Berücksichtigung finden, die von Praxisrelevanz sind. Dies betrifft etwa Verfahren zur Fehlererkennung, Fehlerkorrektur, Datenkompression und Datenfüllung (Padding). Dem Schlüsselmanagement wird eine besondere Aufmerksamkeit gewidmet, zudem werden die aktuellen Entwicklungen im Rahmen der Standardisierung verfolgt.

Ziel der Fachgruppe ist es, ein unabhängiges Forum aus Kompetenzträgern und Anwendern zu bilden. Persönlichkeiten aus relevanten Organisationen (Forscher, Entwickler, Hersteller, Dienstleister, Nutzer, Behörden) haben bereits ihr Interesse bekundet, aktiv in der Fachgruppe mitzuarbeiten. Dabei sollen auch Schnittstellen zu anderen Fachgruppen geschaffen werden, in denen Verfahren der Kryptologie von besonderer Anwendungsrelevanz sind.

Außerdem soll Aufklärung darüber geschaffen werden, was Kryptologie leistet und was sie nicht leisten kann. Dazu könnte schon in naher Zukunft eine Sommerschule Kryptologie eingerichtet werden. Eine Einbettung in nationale und internationale Veranstaltungen (etwa Konferenzen und Messen) ist ebenfalls vorgesehen.

Bei den Aktivitäten der Fachgruppe ist eine enge Kooperation mit den entsprechenden Fachgruppen der Österreichischen Computergesellschaft (OCG), der Schweizer Informatikgesellschaft (SI) und der Informationstechnischen Gesellschaft (ITG) geplant; erste Gespräche dazu haben bereits stattgefunden. Zudem ist eine Zusammenarbeit mit dem Verband BITKOM und dem TeleTrusT Verein sowie den darin organisierten fachspezifischen Unternehmen, dem BSI und weiteren relevanten staatlichen Institutionen ausdrücklich erwünscht.

Zur Information der Mitglieder sollen die relevanten Medien eingesetzt werden, dabei soll neben einer geeigneten Webpräsenz insbesondere ein Druckmedium, etwa die Zeitschrift IT Security, zum Einsatz kommen.

FG Steganographie und digitale Wasserzeichen

Initiatoren:

- Andreas Pfitzmann pfitza@inf.tu-dresden.de
- Jana Dittmann jana.dittmann@ipsi.fraunhofer.de
- Martin Steinebach martin.steinebach@ipsi.fraunhofer.de

Kurzbeschreibung:

Motivation

Digitale Mediendaten haben in den letzten Jahren ein starkes Wachstum erfahren. Sie öffnen neue Märkte und Möglichkeiten: Steganographie und nicht-wahrnehmbare digitale Wasserzeichen (s.u.) haben zwar unterschiedliche Ziele, befruchten sich in ihren Grundlagen und Techniken aber gegenseitig.

Steganographie

Mittels steganographischer Systeme können in digitale Mediendaten Informationen so eingebettet werden, dass nur der intendierte Empfänger sie überhaupt erkennen und danach extrahieren und interpretieren kann. Steganographische Systeme sind in ihrer Wirkung bzgl. Vertraulichkeit umfassender als kryptographische Systeme und auch dann einsetzbar, wenn kryptographische Systeme – etwa in totalitären Staaten – verboten sind und verschlüsselte Daten deshalb nicht übertragen werden.

Digitale Wasserzeichen

Um digitale Mediendaten vor Manipulation, Diebstahl und Fälschung zu schützen, können sie verschlüsselt oder mit versteckten Informationen markiert werden. Nicht-wahrnehmbare digitale Wasserzeichen können zur Sicherung der Authentizität und Unverfälschtheit von digitalen Bild-, Audio- und Videomaterialien sowie 3D-Modellen oder Kombinationen aus diesen Medien verwendet werden. Um Beweissicherheit zu erhalten, müssen sie mit zusätzlichen Diensten wie digitalen Signaturen oder Public-Key-Infrastrukturen kombiniert werden.

Arbeitsziele

Ziel ist es, innovative Verfahren im Bereich Steganographie und digitaler Wasserzeichen zu entwickeln und zu evaluieren.

Für Steganographie besteht die Herausforderung darin, die (Nicht)Erkennbarkeit unter plausiblen Annahmen nachzuweisen oder zumindest den Aufwand für ein Erkennen und/oder seine Unsicherheit zu quantifizieren.

Für digitale Wasserzeichen besteht die Herausforderung in der Entwicklung hinreichend robuster Verfahren, d.h. solcher Verfahren, bei denen das Wasserzeichen nicht ohne störende Verfälschung des Mediums entfernt werden kann. Auf der Basis digitaler Wasserzeichen sind weiterhin Schutzsysteme für digitale Medien zu konzipieren und zu evaluieren. Der Schwerpunkt liegt auf Urheber- und Kundenidentifizierung sowie Manipulationserkennung. Um übergreifende Lösungen zu bieten, sehen wir die Definition von Qualitätsmaßstäben und eine Standardisierung der Prozesse als zwei der Hauptaufgaben.

FG E-Commerce, E-Government und Sicherheit

Initiatoren:

- Rüdiger Grimm ruediger.grimm@tu-ilmenau.de
- Kai Rannenberg kair@microsoft.com
- Martina Rohde martina.rohde@bsi.bund.de

Kurzbeschreibung:

Zwei Aspekte der Sicherheit sind im E-Commerce bzw. E-Government besonders eingehend zu behandeln: erstens die Gefahrenabwehr (vor Viren, Datendiebstahl und –verlust, Maskeraden u.a.m.) und zweitens Sicherheit als eine der wesentlichen Voraussetzungen für jeglichen/jegliches E-Commerce/E-Government, insbesondere auch für ganz neue Anwendungen über das Internet. Die Untergruppe E-*Commerce* & E-Government wird sich vor allem mit dieser zweiten ("enabling") Rolle von Sicherheit für E-Commerce und E-Government befassen.

In dieser "enabling" Rolle ermöglichen Sicherheitsmechanismen der Informationstechnik ganz neue Formen von verbindlicher elektronischer Kommunikation, die ohne sie nicht nur unsicher wären, sondern gar nicht existierten. Dazu gehören z.B. die formalen Anträge und Bescheide im öffentlichen Bereich (Steuern, Grundbuch, Bauanträge usw.) im E-Government sowie die kommerziellen Anwendungen, die unter dem Begriff E-Commerce zusammengefasst werden.

Beispiele für neue E-Commerce-Anwendungen sind elektronische Kataloge, Reiseauskünfte und Buchungen, Kundenbetreuung wie Beschwerden und Reklamationen, und Beschaffungen für den Bereich Business-to-Business. Das Potential der neuen digitalen Medien (Mobiltelefonie, Internet, Digital Broadcast), alle kommunikativen Kanäle im Business-Bereich zusammenzuschalten, stellt das Business vor ganz neue, noch lange nicht erforschte Herausforderungen. Besonders heikel ist der gesamte Finanzsektor. Zugriffe auf Konten (E-Banking) und Bezahlvorgänge (E-Money) sind zwar längst in Gebrauch, aber auf höchst unterschiedliche, teilweise undurchsichtige und oft unsichere Weise. Moderne Sicherheitsmechanismen können hier vereinheitlichend und stabilisierend wirken, wenn sie richtig in die Geschäftsprozesse eingebunden werden.

Beispiele für e-Government-Anwendungen sind elektronische Auftragsvergabe, elektronische Beschaffungsvorgänge, virtuelle Rathäuser u.v.a.m. Als Kommunikationspartner von Behörden als Vertreter der öffentlichen Verwaltung sind sowohl BürgerInnen („citizen"), Unternehmen („business") oder wiederum Behörden selbst („government" oder „administration") anzusehen.

Es bedarf einer großen Anstrengung, in E-Commerce- und E-Government-Anwendungen die notwendige Kundenfreundlichkeit, Sicherheit und das Kundenvertrauen zu implementieren und sie somit für einen Massenmarkt akzeptabel zu machen.

Zentrale Themen für E-Commerce und E-Government sind die Verbindlichkeit von Kommunikation, die Vertragsfähigkeit, die Beweisbarkeit, die Nicht-Abstreitbarkeit und die Revisionsfähigkeit. Selbstverständlich müssen auch Vertraulichkeit und Datenschutz im E-Commerce bzw. E-Government behandelt werden. Ein neues Thema, das der Forschung bedarf, ist die Frage nach dem Vertrauen im Internet. Ebenso stellt sich die Herausforderung Sicherheit von vornherein in die neuen Geschäftsprozesse zu konzipieren, denn einen "papierenen" Prozess erst zu "elektronifizieren" und dann zu versuchen, eben diesen Prozess zu sichern, ist meist zum Scheitern verurteilt. All diese Themen haben interdisziplinäre Bezüge, besonders zur Ökonomie und Rechtswissenschaft. Eine wichtige Partnergruppe innerhalb der GI ist die Fachgruppe 5.5 "E-Commerce" (www.iw.uni-karlsruhe.de/fgecommerce).

FG Datenschutzfördernde Technik (Privacy Enhancing Technologies (PET))

Initiatoren:

- Marit Köhntopp marit@koehntopp.de, koehntopp@datenschutzzentrum.de
- Hannes Federrath federrath@inf.tu-dresden.de
- Simone Fischer-Hübner simone.fischer-huebner@kau.se
- Dogan Kesdogan kesdogan@informatik.rwth-aachen.de
- Astrid Lubinski lubinski@informatik.uni-rostock.de
- Andreas Pfitzmann pfitza@inf.tu-dresden.de
- Rüdiger Grimm ruediger.grimm@tu-ilmenau.de
- Kai Rannenberg kair@microsoft.com

Kurzbeschreibung:

Unter datenschutzfördernden Techniken (engl.: “Privacy Enhancing Technologies (PET)”) versteht man Techniken, die Datenschutz soweit wie möglich fördern und durchsetzen, zumindest aber unterstützen. Borking und Raab definieren 2001 PET wie folgt: “Privacy Enhancing Technologies (PET) are a coherent system of ICT measures that protects privacy [...] by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system.”

Zu den Kriterien und Grundsätzen für PET gehören

- Datenvermeidung und Datensparsamkeit, d.h. die Reduktion personenbezogener Daten in einem IT-System,
- Systemdatenschutz, d.h. bereits technisch im System implementierte und organisatorisch verankerte Datenschutzmaßnahmen,
- Selbstdatenschutz, d.h. ein Maximum an Steuerungsmöglichkeiten durch den Nutzer, sowie
- Transparenz und andere vertrauensbildende Maßnahmen.

Workshops z.B. bei der Europäischen Kommission unter großer Wirtschaftsbeteiligung zu PET zeigen die gestiegene Relevanz des Themas auch und gerade aus unternehmerischer Sicht. Dennoch sind bislang kaum wirkliche PET-Produkte in der Praxis zu finden. Einige gute Ideen bleiben im Ansatz stecken, andere wandeln sich und werden zu Produkten, deren Datenschutzniveau zweifelhaft ist oder die sogar massive Risiken für die Privatsphäre der Nutzer mit sich bringen.

Die PET-Arbeitsgruppe will sich auf verschiedenen Ebenen mit dem Thema PET befassen. Die Ziele der Arbeitsgruppe umfassen:

- Erarbeiten von Klassifikationen, Bewertungsschemata und Bewertungen für PET (auch in Zusammenarbeit mit nationalen und internationalen Projekten für ein Datenschutzgütesiegel),
- Voranbringen von Konzepten und Implementierungen von Bausteinen und Anwendungen für PET (z.B. Systeme für Anonymität und Pseudonymität),
- Abschätzen der Auswirkungen, Möglichkeiten und Grenzen neuer Technologien in Bezug auf Datenschutz,
- Untersuchen von Wechselwirkungen zwischen verschiedenen PET (z.B. Analyse der PET-Eigenschaften auf Robustheit und Kompositionalität),
- Aufbauen auf Ergebnissen von anderen Arbeitsgruppen zu Schutz und Sicherheit,
- Rückmeldungen an andere Arbeitsgruppen über Möglichkeiten von PET in ihrem jeweiligen Kontext sowie
- Veröffentlichung der Ergebnisse auch in allgemeinverständlicher Form und Anstoßen bzw. Befruchten einer politischen Diskussion unter Einbeziehung der Datenschutzbeauftragten.

Zur Mitarbeit sind sowohl Vertreter verschiedener Zielgruppen, z.B. Wissenschaft, Wirtschaft, Verwaltung oder Anwender, eingeladen. Ein interdisziplinärer Ansatz soll neben der Informatik beispielsweise auch Erkenntnisse aus Jura, Ergonomie oder Soziologie einbeziehen.

FG Evaluation, Zertifizierung, Qualitätssicherung, Normung

Initiatoren:

- Kai Rannenberg kair@microsoft.com
- Peer Reymann pr@itqs.de
- Hans von Sommerfeld IT-Sicherheit@t-online.de

Kurzbeschreibung:

Die Komplexität heutiger Informationstechnik macht eine Beurteilung ihrer Sicherheit durch einfache "Draufschau" unmöglich. Entsprechend haben sich verschiedene Verfahren zur Qualitätssicherung und Beurteilung von IT, speziell bezüglich ihrer sicherheitsrelevanten Eigenschaften entwickelt. Im allgemeinen geht es darum, zu sicheren Produkten und Systemen und zu aussagekräftigen, verlässlichen, vergleichbaren und nachvollziehbaren Aussagen über eben diese Sicherheit zu kommen. Im Englischen ist dieser Bereich oft bei "Product/System Security Assurance" angesiedelt, und es ist sehr sinnvoll die "IT-Qualitätssicherung" dabei zu haben, denn die jeweiligen Prozesse kommen mehr und mehr zusammen.

Ein relativ etablierter Weg zu mehr Erkennbarkeit der Sicherheit von IT ist, sie durch unabhängige Dritte (Prüflabors) auf der Basis veröffentlichter Kriterien evaluieren zu lassen. Solche Evaluationen helfen dann auch Nichtexperten, Systeme in Bezug auf ihre Sicherheit und die eigenen Anforderungen einzuschätzen. Hersteller oder Dienstanbieter können in seriöser Weise aufzeigen und prüfen lassen, welche Eigenschaften ihre Angebote haben.

Evaluation und Qualitätssicherung setzen jedoch nicht notwendigerweise unabhängige Dritte voraus, sondern können auch innerhalb der Organisation des jeweiligen Herstellers vorgenommen werden. Möglicherweise lassen sich diese Formen von Evaluation und Qualitätssicherung auch leichter in den Erstellungsprozess integrieren.
Aktuelle Fragen des Gebietes sind z.B.

- Vergleichbarkeit der verschiedenen Evaluationsmethoden und Qualitätssicherungsverfahren sowie deren Ergebnisse. Ein verwandtes Projekt ist das "Framework of IT Security Assurance" (ISO/IEC WD 15443).
- Pflege und Überarbeitung der verschiedenen Evaluationskriterien, etwa der "Common Criteria" (IS15408).
- Protection Profiles auf der Basis von IS 15408, die anwendungsspezifische Anforderungen und Eigenschaften dokumentieren.
- Zugänglichkeit der Prüfergebnisse in einer auch für Nicht-Experten verständlichen Form und über eine geeignete Infrastruktur, etwa die Verbraucherberatungen.
- die verschiedenen Zertifizierungsprozesse mit ihren organisatorischen Randbedingungen: Hier sind z.B. die rechtliche Relevanz und organisatorische Voraussetzungen interessant, auch die Frage der Gültigkeit und internationalen Anerkennung von Zertifikaten.

Das Thema "Normung" ist in vielerlei Hinsicht "orthogonal" zu "Evaluation, Zertifizierung und Qualitätssicherung" wie auch zu Sicherheit allgemein.

Allerdings wird Normung von unterschiedlichen Teilgruppen innerhalb der Sicherheitsszene unterschiedlich wichtig genommen, weswegen sie (einstweilen) dort angesiedelt ist, wo sie unbestritten wichtig ist, nämlich im Zusammenhang mit Evaluation und Zertifizierung.

Normung könnte aber auch durchaus als eigenes Thema verfolgt werden: Zwei erfolgreiche Workshops während VIS 2001 und VIS 1999 sprächen sehr dafür. Praktisch ist es davon abhängig zu machen, wie viele Leute daran zunächst arbeiten wollen.

FG Mobilität und Sicherheit

Initiatoren:

- Astrid Lubinski lubinski@informatik.uni-rostock.de
- Hannes Federrath federrath@inf.tu-dresden.de
- Andreas Pfitzmann pfitza@inf.tu-dresden.de
- Kai Rannenberg kair@microsoft.com

Kurzbeschreibung:

Betrachtet man den Paradigmenwechsel in der Nutzung von Computern, ist Aufmerksamkeit hinsichtlich der HW-Entwicklungen gefordert.

Die Entwicklung verläuft von multifunktionalen Geräten, die obligatorisch auf jedem Schreibtisch zu finden sind, hin zu kleinen, unscheinbaren, tragbaren, integrierten intelligenten Systemen,

- die sogar Alltagsgegenstände “smart” machen,
- neue Interaktionsmöglichkeiten jenseits von Tastatur und Maus haben,
- auf verschiedenste Verhaltensaspekte und Aufenthaltsorte von Menschen reagieren,
- kaum kontrollierbare Kommunikationsbeziehungen pflegen werden und
- mit denen tägliche Abläufe bis zu m-commerce abgewickelt werden.

Was derzeit fehlt, um dem sich ausbreitenden Privacy-Pessimismus zu begegnen, ist eine spezifische Sicherheits- und Datenschutzforschung zu “ubiquitous computing” (UC), die Konzepte entwickelt und zur Nutzung anbietet sowie eine rechtzeitige Begleitung von zukunftsweisenden Forschungsprojekten im Bereich UC.

FG Sicherheit und Zuverlässigkeit softwarebasierter Systeme

Initiatoren:

- Francesca Saglietti saglietti@informatik.uni-erlangen.de
- Karl-Erwin Großpietsch grosspietsch@gmd.de
- Wolfgang Ehrenberger FH Fulda
- Klaus Keus BSI Bonn
- Thomas Rottke TÜV Informationstechnik (TÜVIT) GmbH
- Ernst Schmitter Siemens AG, München

Besonderheit:

Die Fachgruppe soll als Doppel-Fachgruppe des FB 3 (dort FG 3.6.2) und des FB Sicherheit geführt werden.

Kurzbeschreibung:

German ENCRESS, die deutsche Gemeinschaft im europäischen Netzwerk ENCRESS ("European Network of Clubs for Reliability and Safety of Software-Intensive Systems") entstand im Rahmen eines europäischen ESSI-Projekts ("European Systems and Software Initiative"). Ziel des ENCRESS-Netzwerks ist es, den Informationsaustausch unter nationalen und europäischen Arbeitskreisen auf dem Gebiet der Zuverlässigkeit und Sicherheit software-basierter Systeme zu unterstützen. Zu diesem Zweck wurde 1994 die deutsche ENCRESS-Gemeinschaft am Institut für Sicherheitstechnologie (ISTec GmbH, Gar-

ching), dem deutschen Partner des europäischen ENCRESS-Konsortiums, gegründet. Seit 1998 besteht die Gemeinschaft als GI-Fachgruppe FG 3.6.2. Gemäß ihrer Zielsetzung umfasst die Zielgruppe dieser Arbeitsgemeinschaft alle Beteiligten des Sektors, insbesondere Entwickler, Forscher und Anwender, sowohl mit industriellem als auch mit akademischem Hintergrund.

FG Fehlertolerierende Software- oder Anwendungssysteme

Initiatoren:

- Karl-Erwin Großpietsch	grosspietsch@gmd.de
- Mario Dal Cin	Universität Erlangen-Nürnberg
- Elmar Dilger	Robert Bosch AG, Stuttgart
- Erik Maehle	Medizinische Universität zu Lübeck

Besonderheit:

Die Fachgruppe soll als Doppel-Fachgruppe des FB 3 (dort FG 3.6.1) und des FB Sicherheit geführt werden.

Kurzbeschreibung:

Die Fachgruppe beschäftigt sich mit Fragestellungen der Fehlertoleranz in daten- und informationsverarbeitenden Systemen, um den Anforderungen an die Verfügbarkeit, Zuverlässigkeit und Sicherheit bei derartigen Systemen gerecht zu werden. Dabei geht es darum, die Auswirkungen von allen möglichen im System auftretenden Fehlern für nach außen zu minimieren und ein hohes Maß an Datenintegrität zu gewährleisten. Dies beinhaltet sowohl ausfallsbedingte Fehler als auch Entwurfs- und Bedienungsfehler.

Diese Fragestellungen umfassen grundlegende Untersuchungen zur Beschreibung, Architektur, Verifikation und Bewertung derartiger Systeme und die Umsetzung der Erkenntnisse in die Praxis. Dabei ist die FG bemüht, der Vielschichtigkeit der Thematik durch umfassende Information auf allen zuvor genannten Gebieten gerecht zu werden und durch Sammeln und Bewerten von nationalen und internationalen Aktivitäten allen interessierten Fachleuten eine breite Basis zu liefern. Dazu führt sie eigene Fachveranstaltungen durch und gibt Mitteilungen heraus.

FG ADA

Initiatoren:

- Peter Dencker	dencker@aonix.de
- Hubert B. Keller	keller@iai.fzk.de
- Matthias Suilmann	Competence Center Informatik, Meppen
- Michael Tonndorf	CSC Ploenzke AG, München

Besonderheit:

Die Fachgruppe soll als Doppel-Fachgruppe des FB 2 (dort FG 2.1.5) und des FB Sicherheit geführt werden.

Kurzbeschreibung:

Unser Leben hängt zunehmend von der Sicherheit Software/Computer-gesteuerter Systeme ab. Dazu zählen Verkehrssysteme zu Lande, zu Wasser und in der Luft, medizintechnische Systeme, Atomkraftwerke, aber auch Telekommunikationssysteme oder Netzleitsysteme der Stromversorgung. In den Bereichen Verkehr, Gesundheit, Luft/Raumfahrt und Prozesssteuerung, wo Softwarezuverlässigkeit direkt die Sicherheit für Menschen garantiert, ist Ada zu einer bevorzugten Sprache geworden.

In mehreren internationalen Sicherheitsstandards wird Ada explizit als geeignete Programmiersprache aufgeführt. Dazu zählen der IEC 61508, EN 50128 und DO-178B. Die Luftfahrtindustrie z.B. hat mit dem DO-178B einen weltweiten Standard geschaffen, der diese Probleme behandelt und das Airlines Electronic Engineering Committee hat eine Liste von Ada Eigenschaften aufgestellt, die für die Verwendung in Avionik Software besonders geeignet sind.

Ada unterstützt in einzigartiger Weise moderne Analyse, Design und Programmiermethoden. Deshalb erachten wir Ada als die beste Programmiersprache zur Entwicklung großer zuverlässiger Anwendungen mit knappem Kostenrahmen.

Als GI-Fachgruppe will Ada Deutschland technisch-wissenschaftliche Beiträge auf dem Gebiet der Ada-Technologie leisten.

Darüberhinaus hat Ada Deutschland das Ziel, die Aufmerksamkeit der Öffentlichkeit und der Fachwelt auf die Programmiersprache Ada und deren Bedeutung für die Softwaretechnologie zu lenken und die Verbreitung der Ada-Technologie zu fördern.

FB-interner Arbeitskreis FB-Entwicklung

Ein neuer Fachbereich entsteht nicht über Nacht, sondern muss sich im Rahmen vieler kleiner Entwicklungsschritte festigen und formen. Mit der formalen Einrichtung durch das Präsidium wird ein erster Schritt hierzu getan. Weitere Schritte lasten zunächst auf dem Leitungsgremium, das mit der “normalen” (ehrenamtlichen) Vertretung der Fachbereichsangelegenheiten zunächst gut beschäftigt sein dürfte.

Um die Arbeit des Leitungsgremiums bei der Ausgestaltung des Fachbereiches für die erste Zeit zu unterstützen, werden Interessierte im Rahmen eines zuarbeitenden Arbeitskreises – quasi in Stabsfunktion – weitere Entwicklungsschritte diskutieren und vorbereiten. Der Arbeitskreis wird für die ersten “Entwicklungsjahre” eine wertvolle Fundgrube für weitere Ideen sein, soll aber nicht auf Dauer bestehen bleiben.

FB-interner Arbeitskreis Safety- / Security-Webserver

Um der Community Know-how in den Bereichen Sicherheit, Safety und Datenschutz zu vermitteln und auch im deutschen bzw. europäischen Raum eine Vernetzung zu unterstützen, sind in der Vergangenheit entsprechende internetbasierte Projekte entstanden. Ein Beispiel hierfür ist der “Security Server” in Siegen (http://www.uni-siegen.de/security/) und das “Security Gate”, das im Rahmen des DFG-Sonderforschungsprogramms “IT-Sicherheit” entsteht (http://spps.iig.uni-freiburg.de/securitygate/), und das Virtuelle Datenschutzbüro (http://www.datenschutz.de/). Der Fachbereich könnte hier die Initiative ergreifen und einen für die im deutschsprachigen Raum ansässige Community Know-how-Server aufbauen und dabei bestehende Projekte bündeln. Aus Interessierten soll sich hier ein Arbeitskreis bilden, der dieses koordinierend übernimmt.

FB-interner Arbeitskreis FB-Publikationen

Es gibt Fachbereiche mit eigenen Publikationsorganen. Für den neuen FB wäre dies ggf. auch eine interessante Möglichkeit, sich seinen Mitgliedern mitzuteilen. Ersten Signalen zufolge wäre mit der Zeitschrift DuD grundsätzlich eine Zusammenarbeit denkbar. Diese bzw. weitere Alternativen wären zu diskutieren.

Unter Berücksichtigung der in GI-Präsidium und Vorstand derzeit diskutierten künftigen Publikationsstruktur wäre es Aufgabe dieses Arbeitskreises, ein Publikationsmodell für den FB zu entwickeln und mit dem betreffenden Verlag und der GI zu verhandeln. Der FB hätte ggf. auch Möglichkeiten, neue Modelle auszuprobieren, da (noch) keine Verlagsverpflichtungen und vertragliche Verflechtungen bestehen.

4.3 Verhältnis zum Präsidiumsarbeitskreis “Datenschutz und IT-Sicherheit”

Der Präsidiumsarbeitskreis (PAK) “Datenschutz und IT-Sicherheit” hat bislang sehr erfolgreich die Reaktionen der GI auf aktuelle Ereignisse im Bereich von Datenschutz und IT-Sicherheit mitgestaltet, z.B. in Form von Pressemitteilungen. Der PAK besteht aus VertreterInnen verschiedener Fachbereiche und wurde im Jahr 1994 eingesetzt, Sprecher ist Herr Rüdiger Dierstein. Herausragende Merkmale sind die

schnelle Reaktionsfähigkeit und die weitgehende Repräsentation aller Fachbereiche der GI, die durch die derzeitige Organisationsform als Präsidiums-AK gegeben ist.

Es wird vorgeschlagen, den PAK “Datenschutz und IT-Sicherheit” in seiner bisherigen Position beizubehalten, um dessen Arbeit, Präsidium und Vorstand kurzfristig zu aktuellen Themen, den Datenschutz und die IT-Sicherheit betreffend, zu beraten und bei der Öffentlichkeitsarbeit zu unterstützen, nicht zu gefährden, da der im Aufbau befindliche neue Fachbereich diese Aufgabe nicht wirklich wahrnehmen kann. Diese Dualität in den Strukturen findet sich auch in anderen Informatikgesellschaften, z.B. der British Computer Society (BCS).