

Themenschwerpunkt Safety & Security



Fraunhofer
Gruppe
Informations- und
Kommunikationstechnik

Sicherheit serienmäßig

Warum »Homeland Security« innovative IT braucht.....S.5-20

Warum Software nur durch Engineering sicher wird....S.21-31

Die Fraunhofer-IuK-Gruppe

Als größter europäischer Forschungsverbund für Informations- und Kommunikationstechnik (IuK) versteht sich die Fraunhofer-IuK-Gruppe als Anlaufstelle für Industriekunden und Medien auf der Suche nach dem richtigen Ansprechpartner in der anwendungsorientierten IT-Forschung. Die Vernetzung von insgesamt 3.000 Mitarbeitern an 15 Forschungsinstituten sowie zwei Gastinstituten schafft Synergien, ermöglicht anbieterunabhängige Technologieberatung und führt zu branchenspezifischen Lösungen.

Kundenmagazin IuK-News

Die **IuK-News** erscheinen vierteljährlich und können kostenlos abonniert werden. Die in dieser Ausgabe angegebenen »Webkeys« führen im Internet unter www.iuk.fraunhofer.de zu weiteren Informationen und Downloads.

Ein Nachdruck der Texte aus den **IuK-News** ist unter Angabe der Quelle jederzeit möglich (Rücksprache mit der Redaktion erbeten). Neben den in dieser Ausgabe veröffentlichten Bildern und Grafiken kann über die IuK-Pressestelle auch weiteres Bildmaterial kostenfrei zum einmaligen Abdruck bezogen werden.

ISSN 1860-8264

Die Mitgliedsinstitute

- 1 Fraunhofer AIS (Autonome Intelligente Systeme)
 - 2 Fraunhofer FIRST (Rechnerarchitektur und Softwaretechnik)
 - 3 Fraunhofer FIT (Angewandte Informationstechnik)
 - 4 Fraunhofer FOKUS (Offene Kommunikationssysteme)
 - 5 Fraunhofer IAO (Arbeitswirtschaft und Organisation)
 - 6 Fraunhofer IDMT (Digitale Medientechnologie)
 - 7 Fraunhofer IESE (Experimentelles Software Engineering)
 - 8 Fraunhofer IGD (Graphische Datenverarbeitung)
 - 9 Fraunhofer IITB (Informations- und Datenverarbeitung)
 - 10 Fraunhofer IMK (Medienkommunikation)
 - 11 Fraunhofer IPSI (Integrierte Publikations- und Informationssysteme)
 - 12 Fraunhofer ISST (Software- und Systemtechnik)
 - 13 Fraunhofer ITWM (Techno- und Wirtschaftsmathematik)
 - 14 Fraunhofer SCAI (Algorithmen und Wissenschaftliches Rechnen)
 - 15 Fraunhofer SIT (Sichere Informationstechnologie)
-
- a Fraunhofer HHI (Nachrichtentechnik, Heinrich-Hertz-Institut)
 b Fraunhofer IIS (Integrierte Schaltungen)
 * Geschäftsstelle der IuK-Gruppe

Fraunhofer-IuK-Gruppe
 Friedrichstraße 60
 10117 Berlin
 Tel: +49 (0) 30-72 61 56 6-0
 Fax: +49 (0) 30-72 61 56 6-19
 E-Mail: news@iuk.fraunhofer.de

Vorsitzender:
 Prof. Dr. José L. Encarnação
 Stellv.Vorsitzender:
 Prof. Dr. Ulrich Trottenberg
 Geschäftsführer:
 Dipl.-Inform. Boris Groth

Redaktion:
 Alexander Gerber (verantw.)
 Verena Gorris, Jasmin Herbell

Gestaltung:
 Frederike Wagner,
 Julia Solveig Dreyling



Wettlauf von Sicherheit und Technologie



Prof. Jürgen Beyerer
 Leiter des Fraunhofer-
 Instituts Informations- und
 Datenverarbeitung

Sicherheit ist ein Grundbedürfnis des privaten und öffentlichen Lebens. Sie ist ein vielschichtiges Thema von beträchtlicher Komplexität. Der Einsatz von IT-Systemen zur Schaffung von Sicherheit wie auch die Sicherheit von IT-Systemen selbst sind Aufgabenbereiche mit einem hohen Nutzenpotenzial für Menschen, Organisationen und letztlich für die ganze Gesellschaft. Sicherheit ist mehr als nur eine Frage der Technik, gibt es doch in vielen Anwendungsdomänen ausgeklügelte Sicherheitsphilosophien und -strategien, die abgebildet werden müssen, möchte man Sicherheit mit informationstechnischen Mitteln erzeugen oder unterstützen.

Die politische Entwicklung der vergangenen Jahre lässt die Grenzen zwischen privater und öffentlicher, innerer und äußerer Sicherheit und deren Aufrechterhaltung zunehmend verschwimmen. Asymmetrische Bedrohungen in der Grauzone zwischen kriminellen Machenschaften, terroristischen Handlungen und kriegerischen Auseinandersetzungen fordern in aller Konsequenz das ganze Spektrum von privaten über polizeiliche bis hin zu militärischen Vorkehrungen und Maßnahmen. Das gleiche gilt für schwere Natur- und Umweltkatastrophen, denen nur durch Kooperation aller Kräfte adäquat begegnet werden kann. Die Verwischung der oben genannten Grenzen bietet die Chance, Forschungs- und Entwicklungsanstrengungen zu bündeln und Synergien durch wechselseitigen Transfer von Fortschritten zu erschließen. Wie die Wirtschaft selbst die politischen Rahmenbedingungen hierfür einschätzt, lesen Sie in einem Interview mit Fabian Bahr, dem Bereichsleiter Wirtschafts- und Innovationspolitik beim Branchenverband BITKOM, der soeben ein neues Gremium »Homeland Security« ins Leben gerufen hat (ab Seite 29).

Aus wissenschaftlich/technischer Sicht kann man ein komplexes Thema wie Sicherheit nur umfassend angehen, indem man systemtheoretisch allgemeine Prinzipien herauschält, auf deren Basis generische Methoden entwickelt, um daraus schließlich optimale Lösungen für konkrete Aufgabenstellungen ableiten zu können.

Abstrakt gesehen, besteht eine Gefährdungssituation aus einer Gefahrenquelle, einer Gefahrensenke (dem gefährdeten Subjekt oder Objekt) und einem dazwischen liegenden Ausbreitungsweg. Nimmt man das simple Beispiel eines von einem Dach herab (Maßnahme an der Quelle) fallenden Ziegels, so ist das Dach die Quelle und ein Mensch, der vom Ziegel getroffen werden könnte, die Senke. Zur Gewährleistung von Sicherheit könnte man die Ziegel besser befestigen (Maßnahme an der Quelle) die Ausbreitung durch ein Fangnetz hemmen (Maßnahme auf dem Ausbreitungsweg) oder den Menschen einen Helm tragen lassen (Maßnahme an der Senke).

An diesem Beispiel wird klar, dass die beiden Facetten der Sicherheit, die man im Englischen mit Security (absichtlich herbeigeführte Gefährdung betreffend) und Safety (fahrlässig oder zufällig herbeigeführte Gefährdung betreffend) bezeichnet, nur an der Quelle sinnvoll unterschieden werden können. Sobald der Ziegel unterwegs ist, spielt es für die Gefährdung des Menschen keine Rolle mehr, ob er sich zufällig gelöst hat oder absichtlich gelöst wurde. Damit sind, in Bezug auf Ausbreitungsweg und Senke, die gleichen sicherheits-erzeugenden Ansätze sowohl für Security als auch für Safety anwendbar und eine Unterscheidung dort überflüssig.

Aus der Sicht der mathematischen Spieltheorie unterscheiden sich die Aspekte Safety und Security dadurch, dass im ersten Fall der Gegner Natur und Umwelt heißt und mithin naturgesetzliches Verhalten zeigt. Im zweiten Fall ist der Gegenspieler intelligent und versucht absichtlich und geplant zu schaden.

Die Gefahrensenke hat typischer Weise unterschiedliche Flanken der Verwundbarkeit. Es gilt das Minimalprinzip: Für ein minimales Risiko müssen alle Flanken ausreichend geschützt werden. Schadensereignisse, Katastrophen und so weiter sind nicht statisch, sondern sind zeitlich verlaufende Prozesse mit einer Anbahnung, einem Eintreten und mit Konsequenzen. Systeme, die Sicherheit gewährleisten sollen, müssen somit selbst dynamisch sein. Die Erzeugung von Sicherheit muss als Prozess begriffen werden, der entsprechend der Dynamik des gefährdungsrelevanten Geschehens zyklisch beobachtet, entscheidet und handelt, um schließlich erneut zu beobachten, ob die Handlung den gewünschten Effekt erzielt hat. Gleichsam etabliert diese Rückkopplung einen Sicherheitsregelkreis, mit all den bekannten Vorteilen, die Regelungen gegenüber Steuerungen haben. Dass man dabei jede verfügbare Information über das Geschehen nutzt und auch alle Handlungsoptionen systematisch einbezieht ist notwendige Voraussetzung für optimale Entscheidungen eines solchen Systems. Klar ist auch, dass prädiktive Fähigkeiten, wie sie beispielsweise durch mitlaufende Simulationen bereitgestellt werden können, die Leistung sicherheits-erzeugender Systeme steigern können.

Eine fundamentale Rolle spielt die Sicherheit der IT-Systeme selbst. Will man Sicherheit durch Einsatz von IT-Systemen erzeugen, ist die IT-Sicherheit eine notwendige Voraussetzung. Abgesehen von sicherheits-erzeugenden IT-Systemen, kommt der informatischen Flanke der Verwundbarkeit eine stetig wachsende Bedeutung zu. Ist das Terrain dort doch am unübersichtlichsten, die Möglichkeiten für Angriffe extrem vielgestaltig, teilweise von großer Subtilität und einem schnellen Wandel unterworfen. Das macht die IT-Sicherheit zu einer äußerst dynamischen Wissenschaft, die ständig mit dem technologischen Fortschritt und schnell wachsender Komplexität Schritt halten muss.

Zum Schluss erscheint klar, dass Erzeugung und Aufrechterhaltung von Sicherheit mit Hilfe von IT weniger eine Frage von Komponenten als vielmehr eine Frage nach Systemen ist, die erlauben, die Vielschichtigkeit und Komplexität des ganzen Feldes zu beherrschen.

Neben der »sicheren IT« (ab Seite 21) beleuchtet unser Themenschwerpunkt auch die Sicherheit »durch IT« in einem Katastrophenszenario (ab Seite 5).

Ihnen hierbei eine spannende Lektüre!



Foto: ITB

Lebensretter IT

Ein völlig neuer Umgang mit Katastrophen wird möglich

Meist ist die Manöverkritik nach einem Katastropheneinsatz ernüchternd: Gefahren wurden zu spät erkannt und Abläufe falsch vorhergesagt; entschieden wurde gezwungenermaßen auf der Basis ungeeigneter Modellrechnungen und veralteter Datenbestände; die Kommunikation brach zeitweise technisch zusammen oder scheiterte an nicht kompatiblen Systemen. Längst ist die Informationstechnik deshalb unverzichtbar geworden, um Gefahren frühzeitig zu erkennen und abzuschätzen, Risiken zu minimieren und die Katastrophe bestmöglich bewältigen zu können. Die heute bereits eingesetzten Geräte und Verfahren sind allerdings erst der Anfang: Etliche neue Technologien sind jetzt reif für den praktischen Einsatz. Welche IT-Lösungen werden also in den kommenden Jahren Einzug halten ins Katastrophenmanagement? Ein Blick ins Jahr 2010.

Der Hubschrauber hat kaum aufgesetzt, da öffnet sich die Schiebetür – ein ohrenbetäubender Lärm. »Guten Morgen, Herr Minister«, brüllt ein untersetzter Mann und versucht krampfhaft, einen Stapel Unterlagen in seinem Arm festzuhalten, »es ist alles vorbereitet.« Gebückt spurtet der Innenminister unter den Rotorblättern hindurch: »Dann bringen Sie mich mal auf den neuesten Stand, Krause!« Nur mit Mühe kann der Stabschef den großen Schritten seines Chefs folgen. Bernd Krause zieht einen Tablet-PC aus seiner Aktentasche und hält ihn dem Minister vor. »Das Beben setzte vor gut einer Stunde ein, um 3:35 Uhr. Wir müssen davon ausgehen, dass mehrere Tausend Wohnhäuser, vor allem in den nördlichen Vororten, eingestürzt sind, sehen Sie?« Der Minister bleibt vor einer Metalltür stehen. Kein Türgriff, kein Kartenleser, nur zwei kleine Kameras an beiden Seiten.

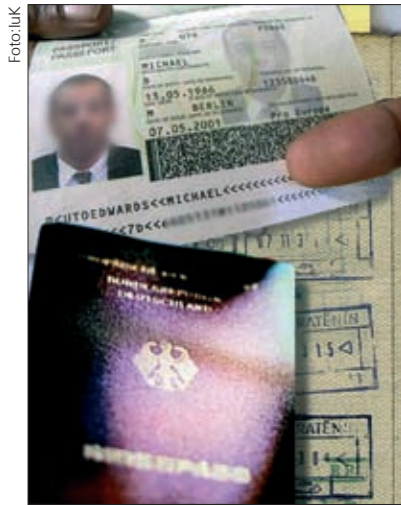


Foto: luK

»Wir betreten jetzt die höchste Sicherheitszone, Herr Minister, bitte einfach einen Augenblick ruhig stehen...« Ein leises Klacken, und die Tür öffnet sich. Der Minister ist irritiert: »Was ist mit meiner Chipkarte? Kommt hier etwa jeder rein?« Krause hält die Tür auf und schüttelt energisch den Kopf: »Ganz im Gegenteil, Herr Minister. Sie haben einen der ganz neuen elektronischen **Ausweise**, einen mit diesem ‚Dual Interface Chip‘, und den kann man sowohl per Lesegerät als auch in Ausnahmefällen, wie hier, drahtlos auslesen. Der Ausweis kann sich außerdem sozusagen selbst verifizieren, das nennt man dann **On-Card-Matching**« Wieder marschiert der Minister mit großen Schritten davon: »Also per Biometrie?« Der Stabschef außer Atem

Bürger haben in punkto Sicherheit »gute Karten«

Wird der elektronische Reisepass bald schon zur »Killerapplikation« für Smartcards?

Darmstadt. Die Pässe der Zukunft sollen biometrische Erkennungsmerkmale wie Fingerabdruck, Gesichtsprofil oder Informationen zur Iris-Erkennung enthalten. Man erhofft sich neben der einfachen Bedienbarkeit – zum Beispiel automatischen Ausweiskontrollen – auch einen enormen Sicherheitsgewinn. Außerdem wird in vielen Staaten angestrebt, die digitalen Ausweise auch als Plattform für die elektronische Signatur zu nutzen, um die Verlässlichkeit im elektronischen Geschäftsverkehr zu stärken. Der Fahrplan steht: Ab November diesen Jahres wird der elektronische Reisepass in seinem Chip zunächst die digitalisierten Daten des Gesichtsbildes enthalten. Ab März 2007 werden in den neuen Pässen zusätzlich zwei Fingerabdrücke gespeichert. Der Stand der Technik ist so weit fortgeschritten, dass elektronische Ausweisdokumente mit Speicherung von Ausweisdaten einschließlich biometrischer Merkmale in digitaler Form realisierbar sind. Als sicherste Speichermedien sind

kontaktlose Chips zu empfehlen. Hier stehen neben einfachen Speicherchips auch intelligente Prozessor-Chips zur Implementierung verschiedener Sicherheitsmechanismen und Zusatz-Funktionen zur Verfügung. Sofern das Format des Ausweisdokuments es zulässt – z.B. bei elektronischen Personalausweisen – empfiehlt sich die Realisierung in Form einer Smartcard. Sollen weitere Funktionalitäten wie Signaturanwendungen mit dem Ausweis ermöglicht werden, empfiehlt sich gegebenenfalls die Verwendung eines so genannten »Dual Interface Chips«, welcher eine kontaktlose und eine kontaktbehaftete Schnittstelle beinhaltet. Im Bereich von maschinenlesbaren Reisedokumenten wurden von der internationalen Luftfahrtbehörde ICAO neben den allgemeinen Anforderungen an die Gestaltung des Ausweises auch schon entsprechende technische Details bezüglich der Datenformate und der Verwendung von PKI-Funktionen zum Schutz der Daten festgelegt.

Der technische Entwicklungsstand im Bereich von Smartcard-Chips und Biometrie und die verschiedenen Vorgaben der ICAO – auch in Bezug auf Anforderungen an den Ausweis-Körper – bieten eine gute gegenseitige Ergänzung. Hierdurch ist insbesondere auch die Möglichkeit der herkömmlichen Ausweisprüfung im Falle eines technischen Defekts beim Ausweis-Chip gewährleistet.

Offene Fragen gibt es derzeit allerdings noch bei der Verwendung extrahierter biometrischer Merkmalsdaten und beim Schutz der Daten gegen unbefugtes Abhören, denn die Standardisierung biometrischer Merkmalsdaten ist noch nicht weit genug vorangeschritten, und die Vorgaben von ICAO zum Schutz der Ausweisdaten sind noch nicht ausreichend. Werden diese offenen Fragen gelöst, werden die zukünftigen Ausweise sicherlich auch von Nutzern und Datenschützern eher akzeptiert werden. [Webkey B0528](#)

hinterher: »Per Gesichtserkennung, ja, aber neuerdings eben **dreidimensional**. Damit ist das System deutlich sicherer und unempfindlicher gegen Störfaktoren.« Am Ende des Gangs hat Krause den Innenminister wieder eingeholt. Ein Offizier salutiert: »Meine Herren, wir haben Sie schon erwartet, der Krisenstab ist versammelt, bitte treten Sie ein.«

High-Security zum Mitnehmen

Identifikation durch biometrische Daten auf der Smartcard

Darmstadt. Sind auf der Smartcard wichtige Daten oder Funktionen untergebracht, sollte sichergestellt sein, dass sich der rechtmäßige Benutzer gegenüber der Karte identifizieren muss. Für diesen Fall eignet sich das so genannte On-Card-Matching. Bei diesem Verfahren findet der Abgleich der biometrischen Daten in der Karte und nicht außerhalb statt. Dies gewährleistet eine große Sicherheit, da die Karte sich bei der Personenkontrolle nicht auf externe Systeme verlassen muss, die manipuliert worden sein können.

Am Fraunhofer SIT wurde auf einer Java-Card-Plattform ein On-Card-Matching-Verfahren für Fingerabdrücke und für handgeschriebene Unterschriften entwickelt. Dieses umfasst auch Lösungen zur Sicherung der Authentizität und Integrität der an der Kartenschnittstelle übermittelten biometrischen Daten. Gerade im internatio-

nalen Umfeld ist jedoch nicht davon auszugehen, dass sich ein einheitliches Verfahren durchsetzen wird. Offene Probleme bestehen auch noch im Bereich der biometrischen Datenformate: Da eine Smartcard keine kompletten Originaldaten (z.B. Bilder), sondern lediglich extrahierte Merkmalsdaten verarbeiten kann, müssen diese in einem standardisierten Format an die Karte übergeben werden. Leider ist die Standardisierung extrahierter Merkmalsdaten noch nicht weit genug fortgeschritten, um die notwendige Interoperabilität in offenen Systemen sicherzustellen. Deshalb überprüfen die Forscher am Fraunhofer SIT in Leistungstests auch andere Implementierungen und führen Interoperabilitätstests für Implementierungen biometrischer Verfahren auf der Basis extrahierter Merkmalsdaten durch, um zu ermitteln, ob sich unterschiedliche Komponenten kombinieren lassen.

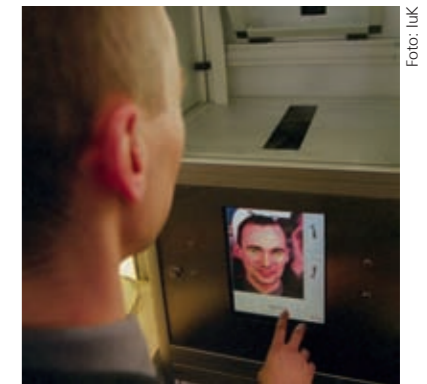


Foto: luK

Dreidimensionale Gesichtserkennung

Darmstadt. Dass die zweidimensionale Gesichtserkennung durch Störfaktoren wie Lichteinfall oder ein Neigen des Kopfes an ihre Grenzen gerät, wurde bereits im Rahmen des Projekts Bioface3 von Forschern des Fraunhofer-Instituts für Graphische Datenverarbeitung gezeigt. Diese Faktoren werden bei der dreidimensionalen Gesichtserkennung eliminiert. Hier wird das Gesicht metrisch korrekt und unverzerrt abgebildet, die Grundmaße wie etwa der Augenabstand bleiben immer gleich. Das Verfahren ist daher sicherer und robuster. Wie gut die bislang entwickelten 3D-Gesichtsscanner in der Praxis wirklich funktionieren, soll eine vom BSI (Bundesamt für Sicherheit in der Informationstechnik) in Auftrag gegebene Untersuchung zeigen. Im Rahmen dieses Tests werden seit Mitte Mai am Bundeskriminalamt in Wiesbaden verschiedene 3D-Gesichtsscanner zur Zugangskontrolle für etwa hundert Mitarbeiter eingesetzt. Geprüft werden die Scanner, unter ihnen auch ein vom Fraunhofer IGD entwickeltes Gerät, auf ihre Leistungsfähigkeit in Bezug auf Qualität und Geschwindigkeit der Erkennung. Erste Ergebnisse werden Ende dieses Jahres erwartet.



Foto: luK

Die Luft in der Katastrophenleitstelle ist stickig. Etwa 15 Leute, in Anzügen, Uniformen oder Einsatzkleidung, stehen vor einem großen **Wanddisplay**, an das unten eine Art Tisch anschließt. Karten und Grafiken, Tabellen, Texte und Luftaufnahmen flimmern über die Wand. Hektik liegt in der Luft. Stimmengewirr, Telefone klingeln. Mit lauter Stimme geht der Minister dazwischen: »Bitte, meine Herren« – die Einzelgespräche ebbeln ab – »wir wollen versuchen, Ruhe zu bewahren. Herr Krause, wie ist die Lage?« Der Stabschef bahnt sich seinen Weg zum Wanddisplay und zeigt auf eine farbig markierte Karte: »Vor etwa 20 Minuten haben wir über dem Katastrophengebiet 350 Sensoren abgeworfen. Wie Sie hier sehen können, haben sich diese Sensoren ad-hoc zu einem Netzwerk verbunden, wodurch wir Informationen über Brände und Rauchentwicklung bekommen. Die Einsatzkräfte sind unterwegs. Die einzelnen Positionen aller Einsatzhelfer können Sie hier unten auf dem Tisch eingblendet in der Karte mitverfolgen. Und um zu erfahren, welche Funktion und Aufgaben ein bestimmter Helfer hat, benutzen Sie einfach diese Tablet-PCs hier.« Krause schiebt über den Lagetisch ein flaches Display, das wie bei einer Lupe einen bestimmten Bereich herauszoomt. Dann markiert er auf einer der anderen elektronischen Landkarten farbig eine bestimmte Stelle: »Hier oben haben wir außerdem einen Staudamm, der nach Einschätzung



Foto: IITB

Im Lagezentrum immer den Überblick behalten

Wie lassen sich größtmögliche Übersicht und Detailschärfe miteinander verbinden?

Karlsruhe. Entscheidend sind bei Umweltinformationssystemen die kartenbasierte Suche und Navigation. Dabei ist die Information größtenteils raumbezogen und muss häufig zur Auswertung im geografischen Kontext mit verschiedenen Medien visualisiert werden – beispielsweise topografischen Karten oder digitalen Landschaftsmodellen. Beim Einsatz von Umweltinformationssystemen im Katastrophenmanagement, insbesondere in der Akutphase, kommt jedoch eine weitere Anforderung hinzu: Unterschiedliche Sichten auf die vorhandene Informationsbasis müssen von verschiedenen Personen unter hohem Zeitdruck gemeinsam ausgewertet werden. Zum Beispiel werden bei ansteigender Hochwassergefahr Experten mit unterschiedlicher regionaler und fachlicher Zuständigkeit in einem Lagezentrum zusammengezogen. Ausgehend von einer integrierten kartografischen Darstellung werden verschiedene Interessengebiete ausgewählt und für

diese Gebiete gleichzeitig Modellrechnungen angestoßen. Deren Ergebnisse müssen in einer Karte zusammengeführt werden, um für eine gemeinsame Entscheidung eine übersichtliche Darstellung zu bieten. Die Kartendarstellung muss einerseits ständig eine Übersicht über das Gebiet präsentieren, andererseits aber auch hochaufgelöste Information an einzelnen Interessenschwerpunkten darstellen.

Gängige Bildschirm-Arbeitsplätze erreichen zwar die erforderliche Detailauflösung an den Interessenschwerpunkten, erschweren aber die Übersicht und eignen sich nicht für die Zusammenarbeit größerer Teams. Großbildschirme oder Projektionen, ob horizontal oder vertikal, erlauben die gemeinsame Übersicht im Team, leiden aber unter schlechter Detailauflösung. Ein digitaler Lagetisch sollte deshalb die Interaktion mit einem geografischen Informationssystem ermöglichen, so dass ein Auge-in-Auge kooperierendes Team von

Experten sowohl eine großflächige Lageübersicht, als auch eine flexibel fokussierbare, ausreichend hohe Ortsauflösung der Interessengebiete erhält. Der am Fraunhofer IITB entwickelte digitale Lagetisch ist als Arbeitsplatz mit einer horizontalen tischartigen sowie einer vertikalen tafelförmigen Anzeige- und Arbeitsfläche ausgelegt. Die Horizontalkomponente dient als Kartentisch und Arbeitsfläche zur Lageübersicht. Sie ist als ca. 1.2 m x 1.6 m große Mattscheibe realisiert, auf welche das Lagebild von unten projiziert wird. Ein vertikaler 45-Zoll-LCD-Bildschirm stellt Seitenansichten des Interessengebiets dar, wie etwa ein Bodenschnittbild mit Grundwasserlagen. Die Ortsauflösung auf dem Tisch-(Karten-) *Display* ist aufgrund geringer Pixeldichte nur für eine Übersichtsdarstellung geeignet. Um diesen Nachteil zu überwinden, wird die vom IITB entwickelte Technik des Fovea-Tablets eingesetzt. Eine kleine, portable Display-Einheit, zum Beispiel ein so genannter

Analyse: Eine Vielzahl von Informationen aus den unterschiedlichsten Quellen muss im Lagezentrum zentral interpretiert werden. Bei der Darstellung müssen größtmögliche Übersicht (rechts) und höchste Detailschärfe (links) unter einen Hut gebracht werden.



Foto: IITB

Tablet-PC, mit hoher Ortsauflösung wird einfach auf den Kartentisch gelegt. Über eine Messvorrichtung wird dessen Lage und Drehung bezüglich des Kartentischs bestimmt. Diese Daten werden drahtlos an das Fovea-Tablet gemeldet, das dann die Kartenabbildung so darstellt, dass die Betrachter den Eindruck haben, sie würden durch das Display hindurch auf die Gesamtkarte sehen, mit einer an dieser Stelle aber wesentlich höheren Auflösung. Neben der besseren Ortsauflösung kann in dem Display auch eine Karte höheren Maßstabs dargestellt werden, die stärker detaillierte Symbole enthält – eine Art digitale Lupe.

Das Fovea-Tablet dient gleichzeitig als Ortstrigger für das Tafeldisplay, welches die vertikale Sicht des Interessengebiets um den Zentralpunkt des Tablets anzeigt. Es ist auf dem Arbeitstisch leicht verschiebbar. So kann jeder Experte aus dem Team seinen Interessenschwerpunkt frei und schnell wählen. Es können auch mehrere

Tablets gleichzeitig eingesetzt werden. Herzstück des Lagetischs ist eine innovative Positionsbestimmung: Jedes Fovea-Tablet trägt auf seiner Unterseite eine Messmarke mit integriertem Nummerncode. Eine Kamera unterhalb des Leuchttischs verfolgt alle Marken der auf der Fläche aufliegenden Tablets. Der Nummerncode identifiziert jedes einzelne Tablet, die Messmarke gestattet eine genaue Positionsbestimmung. Um die Vermessung der Marken von dem auf den Kartentisch projizierten Bild unabhängig zu machen, arbeitet die Messkamera im nahen Infrarot (0,78 - 1,5 µm). Zur Identifizierung und Vermessung kommt das vom IITB entwickelte Multi-Cursor-MarkerXtrackT (MC-MXT) Verfahren zum Einsatz. Die Messmarken haben sich auch in störbehafteter Umgebung bewährt. Es können bis zu 100 verschiedene Marker gleichzeitig erkannt werden. Die Messgenauigkeit der Position ist besser als 0,1 Pixel (< 3 mm), die Drehlage < 2°. Mit einem 2 GHz PC wird eine

Abtastrate von ca. 20 Hz erreicht. Der MCMXT-Tracker-Server arbeitet in einer unabhängigen Kamera-Rechner Einheit als Embedded System mit einer TCP/IP Socket Schnittstelle mit XML-Protokoll. Eine interaktive Bedienung des Systems während des laufenden Betriebs ist nicht notwendig. Die Darstellungssoftware des digitalen Leuchttischs stellt einen MCMXT-Client dar, der die gewünschte Tracking-Information eines Tablets online vom Server zugesandt bekommt.

Dies geschieht in einer ersten realisierten Variante via Bluetooth. Das Bild ist auf dem FT nochmals gespeichert und es wird der entsprechende Ausschnitt berechnet und dargestellt. Soll die Datenhaltung nur auf dem Server geschehen, muss der Ausschnitt für das FT kabellos übertragen werden. Dazu ist ein funkbasiertes WLAN höherer Geschwindigkeit nötig, um einen zu langen Bildaufbau im FT zu vermeiden.

Webkey 30534

der Experten jede Minute brechen kann. Ein Hubschrauber macht hiervon gerade Infrarotaufnahmen. Die Schäden sind hier unten sehr gut zu sehen, wo sich die Kameraschwenks zu einem **Bildmosaik** zusammensetzen. Sie sehen, werden dabei zugleich bewegte Objekte automatisch erkannt und markiert, wodurch wir den Rettungskräften vor Ort genau sagen können, wer wo zu evakuieren ist.« Aus der hinteren Reihe der Zuhörer kommt in militärischem Ton eine Zwischenfrage: »Sagen Sie, wir haben ja hierzulande noch nie ein solches Erdbeben gehabt.

Bildsensorik ohne Tunnelblick

Weglaufen zwecklos: Mit modernster Sensorik lassen sich auch bewegte Bilder auswerten

Karlsruhe. Die meisten Bildauswertungsverfahren arbeiten bisher mit Einzelbildern oder Videobildfolgen von fest installierten Kameras. Immer öfter werden aber bewegte Sensorsysteme luft- und bodengestützt eingesetzt. So sind Videokameras auf schwankenden Masten, fahrenden oder fliegenden Sensorplattformen montiert, um Überwachungsaufgaben oder Übersichtsbilder zu erstellen. Hierfür hat das Fraunhofer IITB verschiedene Verfahren entwickelt, die auf dem gleichen Prinzip beruhen:



Intelligentes Bilder-Puzzle

In Bildfolgen werden die Veränderungen von Bild zu Bild geschätzt und die Bilder so überlagert, dass in Echtzeit ein Panorama oder Mosaik entsteht. Dadurch ist man in der Lage, Überwachungsaufgaben nicht anhand kleiner Videoaufnahmen, sondern mittels Übersichtsdarstellungen durchzuführen. Der bisher übliche Blick der einzelnen Videokamera durchs Schlüsselloch wird mit einer Historie versehen, die es ermöglicht, Bildbereiche genauer zu inspizieren und einen Überblick zu gewinnen. Mit Kameraparametern oder

Kalibrierung muss man sich hierfür nicht auskennen, und auch Zoomen, Rotation und Neigung der Kamera werden automatisch berücksichtigt. Im Katastropheneinsatz ermöglicht diese Technologie einen Gesamtüberblick über die Lage in Echtzeit. Mehrere Schwenks mit der Videokamera über einer Szene reichen bereits aus. Außerdem eignen sich Mosaikbilder auch gut für eine Archivierung, da der Inhalt von Bildsequenzen auf einen Blick im richtigen Kontext erfasst werden kann und nur ein Bruchteil des Speicherplatzes benötigt wird.



Bilder kommen zu Ruhe

Wird von fahrenden oder fliegenden Plattformen aus gefilmt, machen die Bewegungen es oft nahezu unmöglich, die Bilder zu betrachten oder auszuwerten. Gleiches gilt für Kameras, die auf schwankenden Masten installiert sind. Hier rechnet die Software im Videostream die durch die Eigen-Bewegungen erzeugten Bewegungsanteile heraus. Gerade dies ist allerdings bei fahrenden und fliegenden Plattformen nicht gewollt, da das Bild weiterhin der Kameraführung folgen soll. Deshalb werden hier die kleinen schnellen Bewegungen herausgefiltert und nur die

»gröberen« langsamen Kamerabewegungen belassen. Ergebnis ist ein ruhiges Bild, das in Echtzeit berechnet und ausgewertet werden kann. Im Gegensatz zu bereits kommerziell in Camcordern eingebauten Stabilisierungsverfahren, die typischerweise Bewegungen in X- und Y-Richtung kompensieren, kann das am Fraunhofer IITB entwickelte Verfahren auch komplexe Bewegungen wie Rotation und Zoom stabilisieren.



Überwachung bewegter Bilder

Bewegungen bei bewegter Kamera lassen sich auch verfolgen und im Bild sichtbar machen – zum Beispiel bei der Überwachung durch auf Masten montierte Kameras mit Schwenk-Neige und Zoom-einrichtung. Durch die Scanbewegungen der Kamera wird ein bestimmter Bereich abgesucht, und gleichzeitig können unbefugte Personen verfolgt und dann dem Wachpersonal gemeldet werden. Auch in der Verkehrsüberwachung, in der vom Hubschrauber oder Flugzeug aus sich bewegende Fahrzeuge entdeckt und verfolgt werden sollen, wird diese Technologie in Zukunft zum Einsatz kommen.

Fotos: IITB

Deshalb gibt es wahrscheinlich auch keine Evakuierungspläne, oder?« Der Stabschef runzelt die Stirn, sucht den Blickkontakt und antwortet knapp: »Simuliert, Herr Kollege, simuliert! Wir haben das alles am Computer durchgespielt und so alle beteiligten Einsatzkräfte geschult und trainiert – auch für einen solch ungewöhnlichen Fall. Die Situation mag also Neuland für uns sein, das Katastrophenszenario aber ist es nicht. So haben wir beispielsweise sofort systematisch nach Rissen in nahe gelegenen Staudämmen gesucht, und wir kennen dank der Simulationen die Kapazität der Ausfallstraßen.« Doch der Offizier gibt sich mit der Antwort noch nicht zufrieden: »Wir wissen doch noch gar nicht genau, welche Gebiete von einem Dammbbruch überhaupt betroffen sein werden und welche nicht.« Krause lässt sich nicht beirren: »Vielen Dank, ich wollte das gerade eben erläutern. Die Evakuierung ist bereits angelaufen. Und Sie haben natürlich vollkommen Recht, es ist von entscheidender Bedeutung, dass wir uns dabei auf die Zielregion konzentrieren. Zum Glück wurde vor einigen Jahren im Rahmen der Erschließung neuer Gewerbegebiete hier im Norden der Stadt eine komplette **Gewässersimulation** erstellt. So können wir jetzt verlässlich sagen, welcher Teil des Tals von der Flutwelle betroffen ist, welche Kanalsysteme wie viel Wasser ableiten können und so weiter. Sie sehen das hier oben an dieser hochauflösenden Grafik. Die Simulationen offenbarten schon damals Schwachstellen beim Hochwasserschutz, also hat man hier unten gleich zwei Dämme aufgeschüttet.«

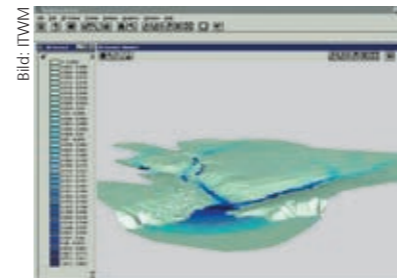


Bild: ITWM

Hochwasser: Auch die Jahrhundertflut im Raum Dresden (rechts) hätte man mit hochauflösenden Computermodellen der Topographie im Voraus simulieren können, um die Risiken für bestimmte Gebiete abschätzen zu können. Fließvorgänge an der Oberfläche und im Kanal lassen sich inzwischen äußerst realitätsgetreu berechnen und darstellen (links).

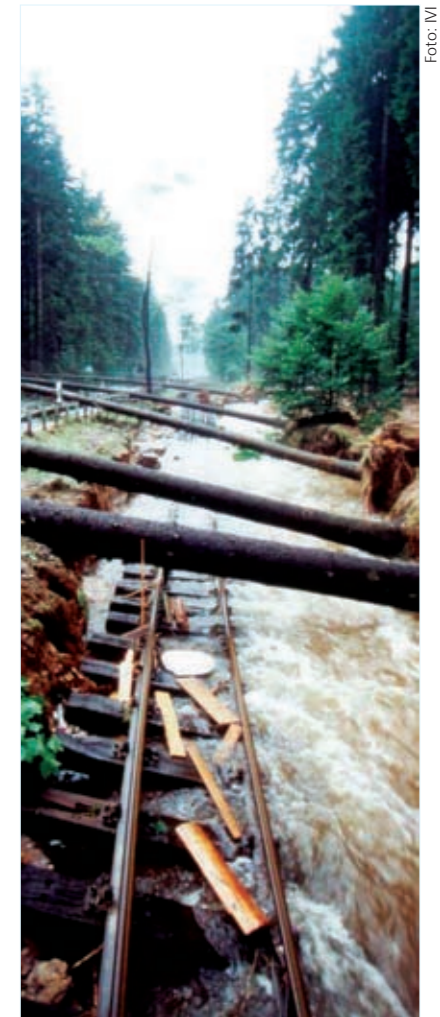


Foto: IM

Simulierte Fluten

Ausgeklügelte Computermodelle für zuverlässige Vorhersagen von Überschwemmungen

Kaiserslautern. Stadtverwaltungen, Einsatzkräfte und nicht zuletzt auch die Versicherer wären brennend daran interessiert, schon lange vor einem Platzregen oder Leitungsbuch genau zu wissen, welches Kanalsystem und welcher Bachlauf ab welchem Zeitpunkt überlastet ist. Nicht nur für die Planung und Erschließung neuer Wohn- und Gewerbegebiete wären solche Informationen bares Geld wert. Doch wie unglaublich kompliziert es in Wirklichkeit ist, den Weg einer Überschwemmung im Computer möglichst realitätsgetreu zu simulieren, zeigt sich erst, wenn man die Vielzahl möglicher Einflussfaktoren betrachtet: Neben Topografie, Gebäudeum-

randungen und Mauern, Dachneigungen und Rohrdurchmessern muss in den Rechnermodellen auch berücksichtigt werden, ob der Untergrund aus Asphalt, Schotter oder Rasen besteht, und ob vielleicht hohe Bordsteine das heranschließende Wasser in eine bestimmte Richtung umlenken. Je detaillierter die Daten im Computermodell umgesetzt werden können, desto verlässlicher ist das Ergebnis der Simulation. Eine am Fraunhofer ITWM entwickelte Software ist in der Lage, extrem hochauflösende Modelle urbaner Topographie zu erzeugen und gekoppelte Berechnungen der Fließvorgänge an der Ober-

fläche und im Kanal durchzuführen. Abschätzungen der Überflutungssicherheit städtischer Gebiete sind somit möglich und bauliche Maßnahmen zur Minimierung des Überschwemmungsrisikos in gefährdeten Gebieten können verlässlicher dimensioniert werden. Oberflächige Überschwemmungen werden häufig von kräftigen, die unterirdische Infrastruktur bedrohenden Anstiegen des Grundwassers begleitet. Ein laufendes Projekt hat daher die Analyse der Wechselwirkung der Fließvorgänge auf der Oberfläche, im Kanal und im Grundwasser und die Ableitung von Vorsorge-maßnahmen zum Ziel. [Webkey 30535](#)

Auch der Vertreter des Technischen Hilfswerks hebt jetzt die Hand, um eine Frage loszuwerden: »Wenn ich das auf der Karte richtig sehe, liegt auch das Chemiewerk mitten in der Gefahrenzone.« Krause blickt zu einem jungen Mann mit Hornbrille hinüber. Dieser räuspert sich und meint: »Ja, das ist leider korrekt. Wir haben allerdings inzwischen direkten Zugriff auf die Firmendatenbank mit allen aktuellen Gefahrenstoffen. Eine eventuelle Ausbreitung bestimmter Stoffe im **Grundwasser** wird gerade am Computer simuliert. In ein paar Minuten müssten uns die Ergebnisse und Grafiken vorliegen. Das sind extrem rechenaufwändige



Foto: IuK

Verlässliche Vorhersagen dank Grid-Computing

Auch die Ausbreitung von Schadstoffen lässt sich inzwischen detailliert und zeitnah simulieren

Berlin. Beim Frontalzusammenstoß zweier Güterzüge explodierte im September 2002 in Bad Münde ein Kesselwaggon. Hochgiftige, krebserregende Gase traten aus, doch die herbeigerufene Feuerwehr konnte nicht löschen, weil keine Informationen über den Inhaltsstoff in diesem Kessel vorlagen. Außerdem wurden falsche Messungen durchgeführt und zu früh Entwarnung gegeben. Tagelang war nicht klar, wie hoch die Belastung des Bodens und der Bevölkerung war.

Präzise Umweltprognosen

Immer wieder zeigt sich bei Katastrophen, dass Gefahren zu spät erkannt und der Ablauf falsch vorhergesagt wurde. Entscheidungen werden auf der Basis unvollständiger und veralteter Daten sowie ungeeigneter Modellrechnungen gefällt, was im schlimmsten Fall viele Menschenleben kosten kann. Katastrophen-Prognosen am Computer sind

allerdings äußerst rechenintensiv, weil zahlreiche Einflussfaktoren berücksichtigt werden müssen, wie etwa Wind, Geologie oder Bebauung. Fraunhofer FIRST hat deshalb mit »ERAMAS« ein internetgestütztes System zum Risikomanagement entwickelt. Durch den Zugriff auf bundesweit verteilte Rechenkapazitäten lässt sich vergleichsweise schnell mit Blick auf eine mögliche oder bereits erfolgte Katastrophe berechnen und darstellen, wie sich Schadstoffe in der Atmosphäre, im Boden und im Grundwasser ausbreiten. Auch der Gefährdungsgrad für die Bevölkerung lässt sich so in kürzester Zeit bestimmen. Eine einfache und intuitiv bedienbare, webbasierte Benutzeroberfläche ermöglicht, dass ERAMAS auch ohne spezielle Kenntnisse der

benutzten Modelle und Methoden produktiv und unabhängig vom Ort eingesetzt werden kann. Das System ist so ausgelegt, dass zu einem späteren Zeitpunkt Modelle von anderen Modellanbietern ohne Probleme eingebunden werden können, um auf diese Weise zum Beispiel neue Simulationsgebiete und weitere Transportpfade in der Simulation berücksichtigen zu können. [Webkey 30537](#)

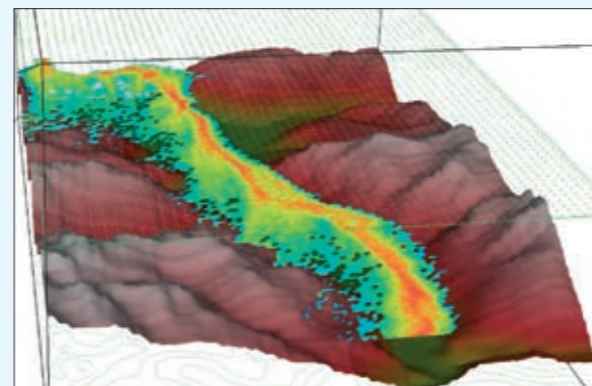


Bild: FIRST

Vorgänge, die nur durch ein Zusammenschalten...« – Krause unterbricht den Kollegen unsanft: »...in ein paar Minuten also, danke, ja. Könnten Sie vielleicht auch noch schnell etwas zur Frage der Kommunikation sagen?« Der Mitarbeiter kramt einen Moment lang vergebens in seinen Unterlagen: »Nun, unsere Einsatzkräfte sind seit Anfang dieses Jahres ausgestattet mit einem neuen **Handfunkgerät**. Neben Digitalfunk und Satellitennavigation sind je nach Einsatzgebiet auch Chipkartenleser, Analysesensoren und Ähnliches integriert. Wir haben in den letzten Jahren ein ganzes Arsenal drahtloser Kommunikationstechnik vor Ort bei den



Foto: ITWM

Mobilfunk-Alleskönner für die Einsatzkräfte

Modulares Handfunkgerät erfüllt die hohen Anforderungen des Schengener Abkommens

St. Augustin. Eines der wichtigsten Hilfsmittel im Katastropheneinsatz sind die Kommunikationsgeräte der Einsatzkräfte. So planen die Behörden und Organisationen mit Sicherheitsaufgaben (BOS), an Stelle des vorhandenen analogen Netzes ein Digitalfunknetz aufzubauen. In Deutschland wird diese Umstellung des Funkbetriebs vielfältig und kontrovers angegangen, auch wenn im Rahmen des Schengener Abkommens bereits wichtige Anforderungen definiert wurden. Expertengruppen haben die Leistungsanforderungen an den Digitalfunk präzisiert und aktualisiert. Gleichzeitig hat die Entwicklung der kommerziellen Digitalfunknetze technisch enorm leistungsfähige Funknetze und mobile Stationen hervorgebracht. Im Auftrag eines Kunden wurden im Fraunhofer AIS Konzept und Prototyp eines Handfunkgeräts für die BOS entwickelt,

in dem einerseits die Anforderungen der BOS laut Schengener Abkommen erfüllt werden, andererseits neue technische Einheiten leicht integriert werden können. Das Gerät wird aus zwei Teilen aufgebaut: ■ Digitalfunk, GPS usw. zusammen mit Bedienelementen, die den Anforderungen der BOS gerecht werden. ■ Einer Ausstattungskomponente mit peripheren Elementen wie etwa Chipkartenleser, Analysesensoren, Fingerabdrucksensor oder Ausweisleser und mit einer zweckmäßigen, leistungsangepassten Bedienoberfläche. Es werden verschieden konfigurierte Ausstattungsteile angeboten, von einer einfachen Anzeigeeinheit für ein Handfunkgerät, bis zu einem Gerät mit Sensoren, Kartendarstellung, Leseinheiten und hochauflösendem Farb-Display. Unabhängig von dem Funkteil kann neue Technologie oder

spezialisierte Ausrüstung auch in kleinen Auflagen bereitgestellt werden. Je nach Einsatzanforderung wird eine passende Ausstattungskomponente gewählt und mit der Funkkomponente zu einem Gerät zusammengesetzt. [Webkey 30529](#)

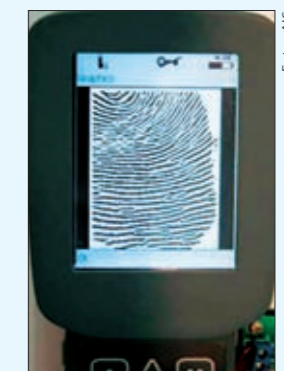


Foto: AIS

Mobil und Flexibel: Das speziell für BOS entwickelte Handfunkgerät lässt sich mit ganz bestimmten Komponenten versehen, wie hier beispielsweise einem Fingerabdruckleser.

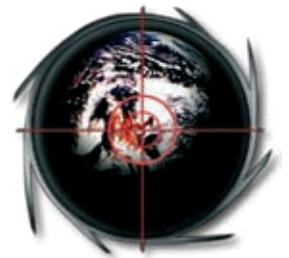
einzelnen Behörden und Organisationen mit Sicherheitsaufgaben getestet, weil ausgerechnet die Kommunikation nicht mit der ansonsten guten technischen Ausrüstung der Einsatzkräfte Schritt gehalten hatte. Analoges Sprechfunk und waghalsige Kurierfahrten mit Martinshorn gehören also inzwischen der Vergangenheit an. Heute haben wir nomadische Informationssysteme, weil die Einsatzkräfte ja ständig in Bewegung sind. Einige Einsatzkräfte arbeiten sogar mit Schutzhelmen und **Spezialkleidung**, die mit ihren integrierten



Foto: FIT

Informationen aufs Handgelenk: In die Kleidung integrierte Computer warnen Feuerwehrleute vor Giftstoffen und anderen Gefahren. Für die Pariser Feuerwehr beispielsweise hat Fraunhofer FIT die Kollaborations- und Informationsprozesse analysiert, um dann eine abgestimmte Wearable-Computing-Unterstützung zu entwickeln. An dem umfangreichen Projekt »wearIT@work« sind insgesamt 37 europäische Partner beteiligt.

Displays, Sensoren und Funkmodulen geradezu wahre mobile Ciomputer sind.« Stabschef Krause hakt vehement ein: »Trotzdem muss man sagen, dass es leider nach wie vor alles andere als selbstverständlich ist, dass wir hier zentral von einem Ort aus auf die Quellen aller relevanten Organisationen zugreifen können. Von unserem zentralen System aus machen sich außerdem kleine Programme, so genannte **Software-Agenten**, auf den Weg, um selbständig Informationen einzusammeln. Die meisten von Ihnen betreiben ja ihr eigenes IT-System, nutzen eigene



Auf Spurensuche mit einem Software-Agenten

Informationsquellen anzapfen mit »Ontologien« in »semantischen Netzen«

Karlsruhe. Die Einsatzleitung benötigt im Katastrophenfall zu allererst ein genaues Bild von der Lage: In welchem Gelände bewegen sich die Einsatzkräfte? Wo sind mögliche Opfer? Welche Schäden sind entstanden? Gibt es noch brauchbare Infrastrukturen? Welche Experten werden benötigt, wo findet man sie und wie sind sie zu erreichen?

Informationen müssen möglichst schnell gesammelt und analysiert werden. Bei der Beschaffung kann sich das Team vom Computer wertvolle Unterstützung holen. So genannte Software-Agenten – kleine Programme, die selbständig im Netz bestimmte Aufgaben erledigen – werden mit einem Suchauftrag über alle verfügbaren Daten und Informationen zum Einsatzgebiet ausgesendet: Sie sollen eigenständig Kartenmaterial, Luftbilder, Beschreibungen besorgen und die Experten kontaktieren. Nur leider verstehen Computerprogramme im Gegensatz zum Menschen zunächst nicht, in welchem Kontext Informationen interpretiert werden könnten. Der Computer braucht also so etwas wie eine

»Unmissverständlichkeit«. Die gesuchten Begriffe, ihre Beziehungen, Eigenschaften und Verflechtungen untereinander (ist Teil von, sieht aus wie, verhält sich wie...) müssen eindeutig festgelegt und beschrieben werden.

Zusammenhänge verstehen lernen

Ein möglicher Zugang zu formalisiertem Wissen sind semantische Netze, die auf der Schlüsseltechnologie der »Ontologien« basieren. Ontologie bedeutet in der Informatik die rechnerinterne Repräsentation und Formalisierung von Wissen damit das Wissen nicht nur vom Menschen, sondern auch vom Computer »verstanden« wird. Ontologien ermöglichen es, Wissen in mehreren Schichten und Sichten zu strukturieren und zu verwalten: verschiedene Wissensgebiete, nutzer- und aufgabenspezifische Ähnlichkeitssichten, Datentypen und Qualitäten werden berücksichtigt.

Unsere Einsatzkräfte erhalten sowohl generelle Informationen über das Einsatz-Gelände als auch über die aktuelle Situation: Wie ist die Topografie und vorhan-

dene Bebauung, welche Infrastruktur ist intakt und benutzbar, wie ist die momentane Wetterlage vor Ort, gibt es Gefahren durch sich ausbreitende Gase? Sind Fahrzeuge im Gelände unterwegs, und wenn ja, welche und wohin bewegen sie sich? Nur wenn diese Informationsquellen »maschinenlesbar« strukturiert sind, kann der Computer seine Unterstützung voll einbringen und den Menschen von der mühsamen Suche entlasten. Der Computer ist zwar »dumm«, dafür aber überaus schnell. Ein ganzer Schwarm von spezialisierten Software-Agenten kann in einem semantischen Netzwerk parallel ausgeschickt bestimmte Suchaufträgen erledigen und wie ein elektronischer Butler seinem Nutzer aufbereiten. Besonders in der Fernerkundung und Aufklärung ist diese Kooperation zwischen Mensch, Netzwerk und Maschine elementar wichtig. Ohne eine exakte Beschreibung der Begriffe und ihrer Beziehungen untereinander gleicht das Netzwerk dem Turmbau zu Babel, und eine maschinenassistierte, aufgaben- und nutzerangepasste Bereitstellung von Wissen wäre nicht möglich.

Schnittstellen, Standards und Dateiformate. Außerdem müssen wir heute wohl noch mit zwei weiteren angrenzenden EU-Staaten Daten austauschen. Zum Glück sind wir in diesem Punkt, der **Interoperabilität**, in den letzten Jahren ein großes Stück weiter gekommen. Im Katastrophengebiet selbst bahnen sich unterdessen kleine mobile Roboter allradgetrieben ihren Weg durch die Trümmer der eingestürzten Häuser. Mit einer Vielzahl fusionierter Sensoren an Bord suchen sie eigenständig nach Überlebenden und erstellen mit einem präzisen 3D-Laserscanner eine dreidimensionale Karte der jeweiligen Unglücksstelle. Dabei sind die Roboter weitestgehend autonom: Sie treffen einen Großteil ihrer Entscheidungen selbst.«

Risiken im Griff behalten

Effizienter Katastrophenschutz verlangt nach aufeinander abgestimmten Info-Diensten

Karlsruhe. Das Elbe-Hochwasser und der Tankerunfall der »Prestige« vor der spanischen Küste im Jahr 2002, Waldbrände im Hitzesommer 2003 und mehrere verheerende Erdbeben in 2004 – immer mehr und immer häufigere Naturkatastrophen haben in den letzten Jahren in Politik und Öffentlichkeit das Sicherheitsbewusstsein erheblich verstärkt. Während die Fachwelt darüber debattiert, welche sozioökonomischen und geowissenschaftlichen Ursachen dafür verantwortlich sein könnten und wie Maßnahmen zur Vorbeugung aussehen, besteht Einigkeit darüber, dass sich Risiken nur dann identifizieren, analysieren und handhaben lassen, wenn Informationen verschiedenster Art, seien es geografische oder thematische Karten, Messwerte, Schadensberichte oder Wettervorhersagen, bereit stehen.

Risikomanagement ist in Europa zumeist Aufgabe öffentlicher Institutionen auf

verschiedenen Verwaltungsebenen, die alle ihre eigenen IT-Systeme zur Bereitstellung von Daten und Diensten betreiben. Die Möglichkeit der teilhabenden Nutzung (sharing) aller relevanten Informationen, insbesondere bei grenzüberschreitenden Naturrisiken, ist dagegen oft sehr begrenzt. Selbst in jenen Fällen, wo der Datenaustausch prinzipiell möglich ist, erschweren unterschiedliche Datenformate und Dienstschnittstellen, aber auch unterschiedliche fachliche Sichten auf das Problemfeld eine schnelle Auswertung der vorliegenden Datenbestände. Sehr viel »Handarbeit« ist notwendig, um die Daten so aufzubereiten, dass daraus verlässliche und belastbare Informationen und Aussagen zur Entscheidungsunterstützung abgeleitet werden können. Das Ende vergangenen Jahres gestartete EU-Projekt »Orchestra« (Open Architecture and Spatial Data Infrastructure for Risk Management) nimmt sich dieser informationstech-

nischen Herausforderung an. Das Ziel des dreijährigen Vorhabens ist die Spezifikation und prototypische Implementierung einer offenen dienstorientierten Software-Architektur. Sie soll das Zusammenspiel der IT-Systeme untereinander – die syntaktische und semantische Interoperabilität – verbessern. Dabei geht es schwerpunktmäßig um Risikomanagement von Naturgefahren (also um die präventive Phase einer Naturkatastrophe). Allerdings ist es das ausdrückliche Ziel des Projekts, die Systemarchitektur so generisch wie möglich zu halten, damit ähnliche Fragestellungen des behörden- und grenzüberschreitenden Managements von Umweltinformationen im Allgemeinen ebenso unterstützt werden können. Insbesondere werden folgende Aufgaben adressiert:

- Analyse der Anwenderanforderungen im Hinblick auf die Funktionalität der Dienste und Informationsbestände



Foto: IITB

Stichwort Interoperabilität: Bei Naturkatastrophen lassen sich die Risiken nur dann zuverlässig und zeitnah analysieren und handhaben, wenn die unterschiedlichen Datenquellen dieselbe Sprache sprechen.

- Entwicklung einer leistungsfähigen und funktional hochwertigen, aber generischen Software-Infrastruktur, um fachbezogene Anwendungsdienste zu ermöglichen, auch über verschiedene Risikobereiche hinweg (Multi-Risk Management, z.B. Überschwemmungen, Erdbeben, Waldbrände oder auch durch den Menschen verursachte Risiken)
- integrierte Betrachtung von raum-, zeit- und sachbezogenen Informationen
- explizite Behandlung von grenzüberschreitenden Aspekten bzgl. Technologie, Verwaltung und natürlicher Sprache
- explizite Modellierung und Nutzung des fachspezifischen Wissens durch einen Ontologie-basierten Ansatz
- Validierung der ORCHESTRA Software-Infrastruktur in praxisnahen, grenzüberschreitenden Anwendungsszenarien
- Einspeisung der ORCHESTRA-Architekturdefinitionen in die Standardisie-

rungsprozesse bei der ISO, beim Open Geospatial Consortium (OGC) und beim europäischen Standardisierungsgremium CEN.

Das Fraunhofer IITB hat im ORCHESTRA-Projekt die federführende Rolle des Software-Architekten übernommen und wird bei der Spezifikation und Implementierung von Kernkomponenten der generischen Software-Infrastruktur mitarbeiten.

Eine wesentliche Herausforderung für ORCHESTRA stellt die Anforderung der EU-Kommission dar, sich mit den folgenden Projekten, denen eine zentrale Rolle im Umwelt- und Katastrophenmanagement zukommt, im Detail abzustimmen:

- INSPIRE – Infrastructure for Spatial Information in the Community, die EU-weite Initiative zur Entwicklung einer europäischen Raumdateninfrastruktur: Da ORCHESTRA neben den fachlichen

Informationsbeständen auch insbesondere Geodaten betrachtet, wird ein signifikanter Beitrag aus ORCHESTRA für die technische Spezifikationsphase der INSPIRE Network Services erwartet.

- GMES – Global Monitoring for Environment and Security, die EU-weite Initiative zur Nutzung von Luft- und Satellitenbildern für die globale Umwelt- und Sicherheitsüberwachung
- OASIS – Open Advanced System for Improved Crisis Management, das integrierte EU-Projekt zur Bereitstellung eines offenen Krisenmanagementsystems

Aufgrund dieses offenen, standardorientierten Ansatzes ist das Ergebnis von ORCHESTRA für das gesamte Themenfeld »Sicherheit« des IITB und der Fraunhofer-Gesellschaft von strategischer Bedeutung.

Webkey B0531

In einigen hundert Metern Entfernung von den Bränden und Explosionen verfolgt die Einsatzleitung die Aktionen der **Roboter** und kann Rettungsteams gezielt mit genauen Ortsangaben zu den Opfern lotsen. Schließlich geht es um Sekunden.

Auch die neueste Generation der Roboter ist im Einsatz: besonders kleine Einheiten, die in Hohlräume vordringen können, die für Menschen völlig unzugänglich sind. Wichtig ist dies vor allem deshalb, weil sich diese Hohlräume oft unbemerkt vergrößern, wodurch darüber liegendes Gestein einbricht und Retter wie Opfer gefährdet werden.

Redaktioneller Hinweis: Abgesehen von den hier beschriebenen Technologien ist die Handlung dieses Katastrophenszenarios selbstverständlich rein fiktiv und folglich Ähnlichkeiten mit tatsächlich lebenden Personen zufällig und unbeabsichtigt.

Aus Robotern werden Retter

Autonome mobile Systeme spüren schnell und sicher Überlebende auf

St. Augustin. Wie lassen sich unmittelbar nach einem Erdbeben oder Terroranschlag mögliche Überlebende in den Trümmern schnell orten und retten? Für menschliche Einsatzkräfte eine gefährliche Mission, weil durch ihr Eindringen in die zerstörten Häuser weitere Zerstörungen verursacht und sie selbst – wie auch die Versütteten – schwer verletzt werden können. Unterstützung erhalten die Einsatzkräfte künftig von Rettungsrobotern: KURT3D ist ein allradgetriebener mobiler Roboter des Fraunhofer AIS, der über mehrere unterschiedliche Sensoren zur Erkundung seiner Umgebung verfügt. Schon bald wird sein Nachfolger klein genug sein, um sogar in Hohlräume vorzudringen, die für Menschen völlig unzugänglich sind.

Roboter liefert räumliche Analyse

Die Ausstattung von KURT3D mit seinen unterschiedlichen Sensoren dient mehreren Zwecken. Zunächst einmal muss sich der Roboter ein Bild des Katastrophenszenarios machen. Dazu hat er nicht nur zwei Schwenk-/Neigekameras an Bord, sondern auch ein am AIS entwickeltes 3D-Sensorsystem, das auf einem Laserscanner basiert. Mit ihm gewinnt der Roboter exakte räumliche Informationen: wie

weit sind Objekte entfernt bzw. welche Ausdehnung haben sie, um aus diesen Daten eine sehr genaue 3D-Rekonstruktion der Umgebung zu berechnen. Dabei wird gleichzeitig die aktuelle Position des Roboters zum Zeitpunkt der Datenerfassung berechnet. Dadurch kann sich der Roboter jederzeit orientieren und auch ohne Fernsteuerung zielgerichtet fortbewegen. Das muss er auch können, denn gerade in realen Katastrophenszenarien ist nicht garantiert, dass eine Fernsteuerung durch den Operateur auch wirklich zuverlässig funktioniert. Drahtlose Kommunikation scheitert oft schon ab der nächsten Hausecke oder wenn der Roboter ins Gebäude vordringt.

Sensoren miteinander kombinieren

Wenn der Roboter autonom nach Versütteten suchen soll, dann braucht er noch weitere Sensoren, wie etwa Mikrophone zur Stimmenerkennung, Wärmebildkameras zum Aufspüren von Körperwärme oder CO₂-Sensoren zur Entdeckung von Atemaktivität. Das zu lösende Problem: kein einzelner dieser Sensoren erbringt vollkommen eindeutige und korrekte Daten, denn bedingt durch Bauart und Umwelt-

einflüsse sind einzelne Sensordaten immer mit Fehlern behaftet. Deshalb bedeutet es eine große Herausforderung, diese Vielzahl von Sensordaten zu fusionieren und daraus zuverlässige Aussagen für die Rettungskräfte in der Leitstelle zu gewinnen.

Robustere und günstigere Roboter

Doch bis solche Roboter in realen Katastrophensituationen zum erfolgreichen Einsatz kommen werden, ist noch weitere Forschungs- und Entwicklungsarbeit nötig. Ziele sind hierbei eine extreme Robustheit, einfache Bedienbarkeit und eine günstige Kosten-/Nutzenrelation des Systems. Ferner ist die Integration des Roboters und der von ihm gelieferten Informationen in die Gesamttechnologie eines Katastrophenmanagementsystems von entscheidender Bedeutung.

»KURT1« baut in Echtzeit 3D-Karten

Auf den RoboCup-Weltmeisterschaften im vergangenen Jahr konnte KURT3D seine Fähigkeiten bereits demonstrieren, in Lissabon wurde er Vizeweltmeister: »Wir waren die ersten, die zeigen konnten, dass Roboter in Echtzeit dreidimensionale Karten bauen können«, erzählt stolz Dr. Hartmut Surmann, Projektleiter beim

Fraunhofer AIS, »und zwar unter wirklichkeitsnahen Wettkampfbedingungen, was schon ein qualitativer Sprung ist gegenüber dem bloßen Laborversuch.«

Im Gegensatz zu herkömmlichen 2D-Abstandsmessern kann das 3D-Sensorsystem, zum Beispiel ein 3D-Laserscanner, überhängende Hindernisse, räumliche Distanzen und die Lage entdeckter Opfer exakt erkennen und bestimmen. Mit seinem Laserstrahl misst der Scanner den Abstand zum Objekt. Er bewegt dabei seinen Laserkopf zuerst horizontal, dann vertikal um 180 Grad. Die Zeit, die der Lichtstrahl braucht, um von einem Objekt reflektiert zu werden, gibt dem Rechner Aufschluss über dessen Entfernung. Dafür braucht er je nach Bildqualität und Raumgröße zwischen zwei und zehn Sekunden. Der Scanner ist mit einer innovativen Software ausgestattet, die ebenfalls vom Team der AIS-Forscher entwickelt wurde. Sie erfasst komplette Oberflächen in Form von dreidimensionalen Punktwolken mit Hilfe verschiedener Echtzeitalgorithmen. Die Echtzeitfähigkeit stellte das größte Problem dar, dem sich die Forscher ausgesetzt sahen: »Aus der großen Gruppe unserer möglichen Algorithmen konnten wir nur sehr wenige verwenden«, erklärt Dr. Surmann.

»Die meisten waren entweder nicht echtzeitfähig oder nicht in der Lage, komplexe Umgebungsinformationen zu berechnen.« Fehlt es vor Ort an Rechenzeit, kann die Software im Bordrechner verschiedene Aufgaben auch noch nach dem Einsatz abarbeiten: beispielsweise die präzise Objektsegmentierung und -erkennung ebenso wie die detaillierte Kartenerstellung. Um diesen Ansatz zur Unterstützung der Einsatzkräfte in Katastrophenszenarien wirklich alltagstauglich zu machen, sucht das AIS beständig den Austausch und die Zusammenarbeit mit Fachleuten für den Katastrophenschutz.

Mini-Roboter vermessen Hohlräume

Ein Weiterentwicklung des Sensorsystems von KURT3D zur Ortung menschlicher Opfer und zur Selbstverortung autonomer Roboter im Gelände ist das nagelneue Mini-3D-Sensorsystem des Fraunhofer AIS: es vermisst Räume mit einem Durchmesser von bis zu acht Metern dreidimensional, dabei wiegt es bei einer Größe von knapp zehn Zentimetern nur noch ein Zehntel seines in Lissabon erfolgreichen Vorgängers, ganze 700 g – besonders wichtig für kleinere und geländegängigere Roboterplattformen wie auch zur

Energieeinsparung an Bord. Damit erschließen sich völlig neue Anwendungsfelder. Nicht nur in Trümmerlandschaften, auch unter U-Bahn-Schächten oder Straßenzügen entstehen häufig kleine Hohlräume, die sich mit der Zeit vergrößern können. Dann besteht die Gefahr, dass der darüber liegende Boden einsackt. Bisher müssen diese Hohlräume mehr oder weniger großflächig aufgebohrt werden – mit hohen Kosten. Mit dem neuen Mini-3D-Sensorsystem können Tiefbauer »minimalinvasiv« arbeiten: Sie bohren lediglich ein Loch von etwa zehn Zentimetern Durchmesser und senken den Scanner ab, um die Gefahr durch den Hohlraum abzuschätzen. Erst dann werden Maßnahmen ergriffen.

Mit dem neuen Mini-3D-Sensorsystem ist ein vielseitig verwendbarer, präziser, flexibler und sehr schneller Sensor für autonome mobile Roboter entstanden. »Ich kenne keinen 3D-Sensor, der so leistungsfähig in der Auswertung ist und gleichzeitig so klein und leicht«, so Dr. Surmann. Da er zudem auch preiswerter als seine Vorgänger ist, profitieren Anwender überall dort, wo schwer zugängliche oder dynamische Umgebungen dreidimensional vermessen oder wo 3D-Modelle erstellt werden sollen.

Webkey 30536



Foto: AIS

Wer ist denn überhaupt mein Gegner?

Warum es wichtig ist, zwischen »Safety« und »Security« zu unterscheiden

»Niemand kommt hier raus, ohne zu bezahlen« schreien die Wachleute, stoßen die Kunden zurück in das brennende Kaufhaus und verriegeln die wenigen noch nicht zugeschweißten Ausgänge. Fast 400 Menschen sterben an diesem heißen Sommertag in Asunción, der Hauptstadt von Paraguay. Glühende Rußpartikel in einem Küchenabzug hatten das größte Einkaufszentrum der Stadt in Flammen gesetzt. Dieses entsetzliche Ereignis wirft ein Schlaglicht auf die beiden Facetten der Sicherheit, die in englischer Sprache trennscharf mit »Safety« und »Security« bezeichnet werden: Security als Sicherheit vor absichtlicher, Safety als Sicherheit vor fahrlässiger oder zufälliger Schädigung. Schon durch das Zuschweißen der Notausgänge bewies der Kaufhausbesitzer, dass er der Security Vorrang vor der Safety gab, seinen Verlust durch Diebstahl mehr fürchtete als Verletzung und Tod seiner Kunden durch Feuer und Rauch.

Die deutsche Sprache kennt mit dem Wort »Sicherheit« nur einen Begriff für die Gewissheit des Menschen, von Schaden verschont zu bleiben. Für diejenigen, den es dennoch trifft, ist es anscheinend zunächst gleichgültig, ob ihm etwas mit oder ohne fremde Absicht zugestoßen ist. Schutzmaßnahmen setzen beim Betroffenen an, härten ihn, machen ihn robust, immunisieren ihn: von der feuerfesten Kleidung über die schussichere Weste, von der Atemmaske bis zur elektronischen Firewall, dem eisernen Vorhang im Computersystem. Solcher Schutz ist immer reaktiv und nimmt sozusagen in Kauf, dass sich die Gefährdung entfaltet. Schutzmaßnahmen haben den Vorzug, dass sie genau auf die verwundbare Flanke zugeschnitten werden können. Ihr Nachteil ist, dass sie

immer mitgetragen werden müssen – in Erwartung einer möglichen Gefahr, obwohl sie vielleicht nie gebraucht werden.

Je näher man zur Quelle der Gefährdung vordringt, desto wesentlicher ist es, Absicht und Zufall, Security und Safety zu trennen. Sicherheit an der Gefahrenquelle herzustellen, ist Gefahrenabwehr, ist proaktiv, bedeutet das Erkennen und Neutralisieren einer aufkommenden Gefahr. Es öffnet die Sicht auf einen zyklischen Prozess zur Gewährung von Sicherheit: vom Erkennen der Gefahr über das Entscheiden für Maßnahmen zum Schutz und zur Abwehr und deren Umsetzung zurück zum Erkennen des Erfolges. Dieser Prozess kann in drei Phasen angewendet werden: präventiv, akut oder rehabilitierend. In der präventiven Phase wird eine Gefährdung nur vermutet, und es werden vorsorgliche Maßnahmen ergriffen. In dieser Phase besteht Unsicherheit über das tatsächliche Gefahrenpotenzial. Eine zuverlässige Einschätzung ist hier wesentlich, um nicht in allgegenwärtigem Gefahrenverdacht zu erstarren. In der akuten Phase dagegen ist die Gefahr gegenwärtig und klar. Hier kommt es wesentlich auf schnelle und entschiedene Reaktion für Schutz und Gegenwehr an. Die rehabilitierende Phase tritt dann ein, wenn sich die Gefahr bereits entfaltet hat; sie soll den Schaden begrenzen. Dafür ist eine robuste Organisation der Maßnahmen gefragt, die sich auch durch katastrophale Schadenswirkung nicht aus der Übersicht bringen lässt.

Um einer Gefahr aktiv zu begegnen, muss man ihre Ursache verstehen. Dies gelingt dann verhältnismäßig gut, wenn die Fehlerursache eine zufällige ist – seien es Naturphänomene wie das Wetter oder

das Versagen von Menschen und technischen Apparaten. Je besser man durch Forschung eine Zufallsquelle von Gefahren zu verstehen lernt, desto zielgenauer kann man an der Ursache ansetzen, diese rechtzeitig erkennen und Gegenmaßnahmen einleiten. Es ist ein »Spiel« gegen die Natur, auch die fehlbare Natur des Menschen. Dieses Spiel kann man auf lange Sicht gewinnen. Der Sicherheitsprozess konvergiert. Über kurz oder lang kann eine weitgehende Automatisierung des Sicherheitsprozesses erreicht werden.

Ist der Gegenspieler aber ein Mensch, der schädigen will, konvergiert der Prozess nicht. Hier stehen wir im Feld der Security, im »Spiel« gegen einen Gegner, der sich dem Verstandenwerden entziehen will, der sich tarnt, der täuscht. Hier greifen technische Lösungen zur Gefahrenerkennung und -abwehr nur eine Zeit lang; nämlich so lange, bis der Gegner die Regeln der Gegenmaßnahmen durchschaut und sein Verhalten ändert. Gefahrenerkennung und -abwehr bei Security-Bedrohung ist geprägt vom Aufeinanderprallen menschlicher Interessen. Sie bedürfen der aktiven und andauernden Anstrengung des Menschen im Sicherheitsprozess.

Technische Hilfsmittel sind dabei unerlässliche Werkzeuge, die vor allem die Wahrnehmung der Gefahrenlage entscheidend verbessern helfen. Um aber Security-Bedrohungen zu begegnen, stehen sie im Dienste von Menschen, die diese zwischenmenschlichen Konflikte austragen und deren wesentliche Interaktion mit dem technischen Hilfsmittel vor allem darin besteht, dieses in einem ständigen Anpassungsprozess für die Auseinandersetzung mit einem Gegenspieler fit zu machen.

Bild: IITB

Sicherheit serienmäßig

Von der Ausfallsicherheit übers Krisenmanagement bis zur Schadensbegrenzung

IT-Systeme vor krimineller Energie zu schützen, ist die eine Seite der Medaille. Die Ausfallsicherheit des Systems ist die andere. So schafft es noch lange keine nachhaltige Sicherheit, Software mit »Patches« oder teuren Rückrufaktionen nachzurüsten. Sicherheit muss vielmehr von vornherein als Grundbaustein der Entwicklung mit eingeplant werden. Im Ernstfall lässt sich durch ein Störfallmanagement der Schaden minimieren. Ist es auch dafür zu spät, muss zumindest die IT-Forensik Licht ins Dunkel bringen. Die nächsten Seiten geben einen Überblick zum Stand der IT-Sicherheitsforschung.

Spektakuläre **Kriminalfälle** im Zusammenhang mit Computerbetrug oder -sabotage, Meldungen über gravierende softwarebedingte Fehlfunktionen, beispielsweise von Autos oder Flugzeugen – all dies führt uns fast täglich die beiden Facetten der IT-Sicherheit vor Augen: Auf der einen Seite schützen wir Softwaresysteme vor böswilliger Manipulation (Stichwort »Security«), auf der anderen Seite muss die Betriebssicherheit im technischen Sinn sichergestellt sein (Stichwort »Safety«).



Bild: iuk

Cybercrime: Geschätzte 100 Milliarden Euro Schaden

Polizeiliche Kriminalstatistik ist besorgniserregend, zeigt aber nur die Spitze des Eisbergs

Berlin. Computerkriminalität in Deutschland ist innerhalb eines Jahres um 12,2 Prozent auf insgesamt fast 67.000 erfasste Fälle gestiegen. Die Dunkelziffer ist allerdings nach Einschätzung des BKA beträchtlich. So werden Vorfälle oft gar nicht als böswillige Angriffe erkannt, sondern als technische Probleme fehlinterpretiert. Außerdem fürchten viele Unternehmen einen Imageverlust, falls Sicherheitslücken bekannt würden. Der gesamtwirtschaftliche Schaden durch Computerkriminalität ist deshalb nur schwer abzuschätzen. Die Kreditversicherung Euler Hermes beziffert den Schaden auf bis zu 100 Milliarden Euro jährlich. Überdurchschnittlich stark scheint hiervon der Mittelstand betroffen zu sein: Eines von drei mittleren Unternehmen ist in den vergangenen drei Jahren Opfer eines bedeu-

tenden Falls von Computerkriminalität geworden. Dabei gingen drei Viertel dieser Fälle auf das Konto der eigenen Mitarbeiter. Zum ersten Mal erfasst die kürzlich erschienene polizeiliche Kriminalstatistik auch das Internet als »Tatmittel«, also beispielsweise die Nutzung von E-Mails für die Verbreitung pornographischer Schriften oder Sabotage. Von diesen insgesamt knapp 55.000 Fällen wurden mehr als 83 Prozent aufgeklärt. Vergleichsweise niedrig ist die Aufklärungsquote bei der Sabotage (61 Prozent), besonders hoch bei Urheberrechtsverletzungen (94 Prozent). Das Computer- beziehungsweise Internetstrafrecht wurde 1986 eingeführt. Folgende Gruppen von Straftatbeständen werden hierbei unterschieden: Computerbetrug beziehungsweise Betrug im Internet (§ 263a StGB), Verletzung geschützter

Daten (§ 202a StGB Ausspähen von Daten), Datenveränderung (§ 303a StGB) und Computersabotage (§ 303b StGB), Urkundenfälschung im Computer (§ 267 StGB Urkundenfälschung, § 268 StGB Fälschung technischer Aufzeichnungen, § 269 StGB Fälschung beweiserheblicher Daten, § 271, § 274 Abs. 1 Nr. 2, §384a StGB Falschbeurkundung/Urkundenunterdrückung) sowie sonstige Computer- und Internetdelikte (§ 265a StGB Erschleichen von Leistungen, § 317 StGB Störung von Telekommunikationsanlagen). Spamming, Phishing (das Ausspähen von Passwörtern), Cyberstalking, Cyber-squatting (Reservierung von Domain-Namen, die zu einem vielfachen Preis verkauft werden) und Domain-Hijacking sind anstehende Themen für die Detaillierung des Strafrechts.

Bilder: IuK



Gefahrenlevel im »Homeland«: Fünf Stufen hat die Bedrohungs-Skala des US-amerikanischen Ministeriums für Heimatschutz (Department of Homeland Security, siehe unten). Bürger sollen damit auf die aktuelle Gefahrenlage hingewiesen werden. Bei Redaktionsschluss stand die Ampel auf »Gelb«, was einem aktuell »signifikanten Risiko für Terroranschläge« entspricht.



Obwohl das Bewusstsein für die diversen Sicherheitsprobleme, die unsere vernetzte, IT-basierte Welt mit sich bringt, allmählich steigt, kommt die professionelle, sichere Softwareentwicklung immer noch zu kurz im Vergleich zur immensen wirtschaftlichen und auch gesellschaftlichen Bedeutung, die Software heute insbesondere in eingebetteten Systemen innehat.

Angesichts immer mehr vernetzter Systeme, Update- und Fernwartungsfunktionen bieten sich dem potenziellen Angreifer auch immer mehr **Einfallstore**.

Anstatt aber die Softwareentwicklung grundlegend auf systemimmanente Sicherheit auszurichten, wird versucht, durch teure nachträgliche Korrekturen (zum Beispiel über vom Anwender einzuspielende »Patches«) die Sicherheitslücken zu flicken.

Softwaresicherheit muss mehr sein als ein weiteres Verkaufsargument

Flickschusterei ist nicht nur arbeitsaufwändig und kostenintensiv; sie birgt auch zusätzliche Risiken und zahlreiche Fehlerquellen. Ein grundsätzlich sicheres System entsteht so nicht – nicht selten wird sogar das Gegenteil erreicht. Doch der hier beginnende Teufelskreis kann durch eine durchgehend sicherheitsorientierte Software- und Systementwicklung erfolgreich durchbrochen werden. Sie integriert bewährte Verfahrensweisen des Secure Software Engineering in alle Phasen des Entwicklungszyklus – angefangen von der Anforderungsanalyse über den Architekturentwurf und die Implementierung bis hin zum Test des fertigen Systems.

So entstehen Computerprogramme, durch die sich Sicherheitsüberlegungen hindurch ziehen wie der sprichwörtliche »rote Faden«. Nach derzeitiger Erfahrung

Wie verwundbar sind unsere Infrastrukturen wirklich?

Wie in den USA gibt es bald auch in Deutschland eine Stelle für den Schutz kritischer Infrastrukturen

Kaiserslautern. Wenn Strom oder Telefonleitungen ausfallen, Flugsicherungs- oder Verkehrsleitsysteme zusammenbrechen, dann geht oft gar nichts mehr. Was viele aber nicht wissen: Verursacht werden solche großen Störungen oft durch Schwächen in der Informationstechnik selbst. So brachte beispielsweise ein Softwarefehler den Betrieb des Londoner Flughafens Heathrow für einen ganzen Tag zum Erliegen, weil das entsprechende Programm nicht mehr gestartet werden konnte. Die Tragweite dieser

Problematik wird umso deutlicher, wenn man sich vergegenwärtigt, dass solche Ausfälle bislang in der Regel nicht auf gezielte Angriffe zurückzuführen sind, sondern durch unbeabsichtigte Pannen entstehen. Das Schadenspotenzial von gezielten technischen Angriffen mit terroristischem Hintergrund wird deshalb noch weit höher eingeschätzt – ein wichtiger Grund für mehr Forschung zur IT-Sicherheit. Begonnen hat diese Tendenz in den USA, wo George Bush als Reaktion auf die Ereignisse des 11. September das Ministerium

für Landessicherheit / Heimatschutz schuf (Department of Homeland Security).

Zu den Hauptaufgaben der Behörde zählt auch die Entwicklung von Strategien zum Schutz amerikanischer IT-Systeme. Ähnliche Aufgaben wird demnächst auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) übernehmen. Wie Bundesinnenminister Otto Schily ankündigte, soll das BSI zur zentralen Stelle für den Schutz kritischer IT-Infrastrukturen ausgebaut werden und einen Masterplan erarbeiten. **Webkey 30527**

lässt sich Sicherheit im Sinne von »Security« in einem bestehenden System nicht nachrüsten wie etwa ein zusätzliches Leistungsmerkmal. Sie sollte das Entwicklungsprojekt regelrecht durchdringen – am besten unter der Anleitung einschlägiger Experten und über alle Entwicklungsphasen hinweg.

Das größte Sicherheitsrisiko sind Einsparungen bei der Entwicklung

Nicht nur mangelndes Bewusstsein, Kostendruck oder Unkenntnis verhindern konsequent sicherheitsorientiertes Software Engineering und öffnen damit Datenspielen, Cyberterroristen und Computerbetrügereien Tür und Tor. Auch neuere Entwicklungsmethoden können den einschlägigen Sicherheitsempfehlungen zum Teil deutlich entgegenwirken. Generische Programmmodule oder Erweiterungsschnittstellen beispielsweise, deren konkrete Funktionalität erst zur Laufzeit endgültig festgelegt wird, sind zwar universell verwendbar und sparen Entwicklungsressourcen durch Wiederverwendung, ermöglichen jedoch ohne weitere Absicherung auch Angreifern die Nutzung des Systems durch Ausführung fremden Codes. Ein anderes Beispiel ist die weit verbreitete Praxis des Zukaufs externer Komponenten, die nicht selten ohne Detailkenntnis oder -prüfung in **Entwicklungsprojekte** eingeführt und verwendet werden. Was wirtschaftlich durchaus sinnvoll erscheint, birgt nachvollziehbare Sicherheitsrisiken im Bezug auf die Vertrauenswürdigkeit solcher COTS (Commercial Off-the-Shelf)-Komponenten, mit denen letztlich die Gesamtsicherheit des Systems im Bezug auf Manipulationsversuche steht und fällt. Dies bedeutet keineswegs, dass zur Herstellung angriffssicherer Software auf moderne Entwicklungsverfahren grundsätzlich verzichtet werden müsste. Wichtig ist aber auch hier ein Problembewusstsein und die richtige Fachunterstützung, um



Bild: SIT

Sicherheit als Exportschlager

Initiative will den Erfolg bei internationalen Ausschreibungen steigern

Darmstadt. Gemeinsam mit zahlreichen Unternehmen der IT-Branche hat das Bundesministerium für Wirtschaft und Arbeit den Startschuss zur Exportinitiative »IT-Security Made in Germany« gegeben. Mit dieser Initiative wird ein Netzwerk zur Förderung der Exporte deutscher IT-Sicherheitsprodukte, -lösungen und -dienstleistungen geschaffen. Fraunhofer SIT hat den Aufbau des Exportnetzwerks übernommen und unterstützt die beteiligten Unter-

nehmen bei ihrem Engagement im Ausland. Ziel von »IT-Security made in Germany« ist es, die Exportaktivitäten deutscher IT-Sicherheitsunternehmen zu bündeln und ausländischen Interessenten die Informationen zu deutschen IT-Sicherheitsanbietern über eine zentrale Anlaufstelle zugänglich zu machen. »Mit Hilfe des Internetportals können Unternehmen sich und ihre Produkte und Dienstleistungen international präsentieren und gleichzeitig national nach

geeigneten Partnern für Exportbemühungen suchen«, sagt Dr. Rolf Reinema, stellvertretender Institutsleiter am SIT. Nicht nur der Export soll gestärkt, sondern auch der Erfolg bei internationalen Ausschreibungen verbessert werden. Außerdem werden über das Portal zukünftig auch Informationen über Exportbedingungen in den Zielregionen bereitgestellt. Hierzu zählen der arabische Raum, Mittel- und Osteuropa sowie Südostasien. **Webkey 30530**



Mailflut: Jahrelang liefen kontinuierlich etwa eine Million E-Mails pro Monat über den Backbone der Fraunhofer-Gesellschaft. Innerhalb von weniger als einem Jahr (im Schaubild die Jahre 2003 und 2004) stieg die Zahl der E-Mails um mehr als das 20-fache und liegt seitdem bei etwa 25 Millionen. Verantwortlich für diesen rapiden Anstieg waren insbesondere unerwünschte Werbemails – Spam.

angemessene Kompromisse und wirkungsvolle Gegenmaßnahmen finden zu können. »Security by Design« wird vor dem Hintergrund komplexerer Systeme, unzähliger Realisierungsvarianten und immer geschickter agierender Angreifer eine Herausforderung bleiben.

IT-Sicherheit wird zum Herzstück der Unternehmenssicherheit

In allen Unternehmen droht ein Problem, das die meisten bis jetzt eher als »lästig« abgetan haben, die gesamte E-Mail-Kommunikation lahmzulegen: Unerwünschte E-Mails (»Spam«) machen inzwischen 80% des gesamten Datenverkehrs aus und führen zwangsläufig zum »Stau«. Im Gegensatz zur Reaktion vieler Unternehmen, nämlich sich mittels Filtern einzumauern, gibt es auch andere Strategien. Die Mail-Server der Fraunhofer-Gesellschaft beispielsweise nehmen zunächst alle Nachrichten an und analysieren erst dann die komplette E-Mail.



Junk E-Mail [1428]

Mittlerweile sind vier von fünf Mails nur noch Müll

Rettung dank Ritterrüstung oder Suche nach Edelsteinen? Wie Fraunhofer Spam bewältigt

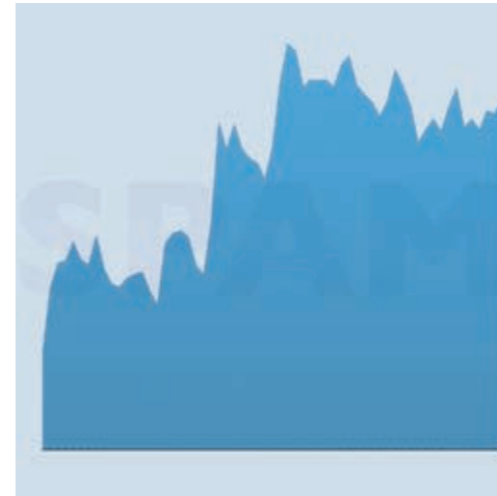
Karlsruhe. Über den zentralen E-Mail-Backbone der Fraunhofer-Gesellschaft, betrieben vom Network-Operation-Center (NOC) des Fraunhofer IITB, werden für rund 10.000 Mitarbeiter ein- und ausgehende Mails vermittelt und auf Viren sowie Spam geprüft. Stagnierte das monatliche E-Mail-Aufkommen bis Frühjahr 2003 bei rund einer Million, stieg es in den folgenden 12 Monaten rapide an und liegt heute bei über 23 Millionen. Die monatliche Anzahl der Virenbehafteten Nachrichten wächst in diesem Zeitraum um den Faktor 40 auf jetzt 400.000. Die Steigerung des Mailaufkommens ist vor allem auf unerwünschte Massenwerbemails zurückzuführen. Zwischen 75 und 90 Prozent der von außen eingelieferten Nachrichten sind als Spam einzustufen. Zwar geht von Spam-

E-Mails per se keine mit Viren vergleichbare Bedrohung aus; doch technisch betrachtet unterscheiden sich die unerwünschten Wurfungen nicht von den täglich millionenfach verschickten E-Mails regulären Inhalts. Es ist die schiere Unmenge der Werbebotschaften, die für jeden einzelnen zunehmend die Kommunikation über das elektronische Medium erschwert. Wie bei einer Telefonverbindung mit starkem Hintergrundrauschen droht der Informationsaustausch im Spam unterzugehen.

Anwender erwarten heute von ihrem IT-Dienstleister Möglichkeiten, die Spamflut in ihrer Mailbox einzudämmen. Computerviren möchte man frühzeitig erkennen und so ihr Gefährdungspotenzial minimieren. Mit dem aufkommenden

Wunsch nach Anti-Spam-Maßnahmen übertragen Anbieter diese Strategie auf unerwünschte Werbemails. Einen ersten Schritt bilden »Schwarze Listen« derjenigen, die in der Vergangenheit Spam-Mails versandten. Entsprechend konfiguriert verweigern Mail-Server die Annahme von Mails eines Absenders oder Rechners, wenn dieser in einer der zahlreichen, im Internet öffentlich zugänglichen, Listen vermerkt ist. Durch bereits simple Variationen der Absenderadressen wird der Ansatz aber wirkungslos.

Um dem entgegenzuwirken, sperren viele Betreiber statt eines einzelnen Absenders oder Rechners komplette Domains. Ein Katz-und-Maus-Spiel beginnt. Es entsteht eine Spirale, in der Empfänger immer rest-



Stauwarnung vom Server: Sprunghaft stieg der Spam-Anteil Mitte 2004 von bis dato knapp 40 % auf jetzt mehr als 80 %. Von je fünf E-Mails sind somit nur noch eine »Ham« und vier »Spam« (im Schaubild die Entwicklung innerhalb von nur zwei Monaten). Fraunhofer-Forscher tüfteln an Strategien, um dieser Flut Einhalt zu gebieten.



Bedrohung durch Viren: Bis zum Sommer 2003 zählten die Fraunhofer-Server meist weniger als 10.000 Viren-verseuchte E-Mails pro Monat. Diese Zahl schnellte im September 2003 auf fast 250.000 und nach einer nur kurzen Erholungsphase im Juni 2004 auf insgesamt 675.000. Seitdem werden jeden Monat mehrere hunderttausend Viren-mails von den Fraunhofer-Servern abgefangen.

riktivere Maßnahmen gegen die Versender von Werbemails ergreifen. Mancher sieht gar das globale E-Mail-System in Gefahr und zieht in einen »Kreuzzug« gegen Spam. Aber ist ein Ritter, der mit seinem Schwert sofort auf alles Verdächtige einschlägt, die richtige Antwort auf Werbemails?

Der Ritter konzentriert sich auf seine Verteidigung, seine Rüstung macht ihn schwerfällig. Dem Ritter tritt man nicht zu nahe. Gleiches gilt für Geschäftspartner, wenn sie Kundenanfragen mit Spam-Vermerk zurückweisen. Für seriöse E-Mail-Dienstleister scheidet ein solcher Ansatz, bei dem die Spam-Bekämpfung wichtiger als die elektronische Kommunikation ist, aus. Der Spam-Schutz des Fraunhofer-Mail-Backbones basiert auf einem entgegen-

gesetzten Ansatz. Die Fraunhofer-Server nehmen alle Nachrichten an. Die Identifikation von Spam erfolgt zu einem späteren Zeitpunkt, dann durch Analyse der kompletten Mail mit Hilfe von spezieller Software. Zurzeit kommt im Fraunhofer-Mail-Backbone »Spam-Assassin 3.0« zum Einsatz, die Klassifizierung justiert das NOC durch eigene Beispielmails nach. Voraussetzung für diese Politik sind ausreichende Ressourcen, die auch bei Lastspitzen die Bearbeitung einer Mail im Sekundenbereich gewährleisten.

Das NOC hat daher 2004 den Mailbackbone um drei zusätzliche leistungsfähige Server erweitert. Die Investitionen in Hardware zahlen sich aus: Viren- und Spam-Erkennung werden von jeweils speziell qua-

lifiziertem Personal gepflegt. Die wenigen von Fraunhofer-Mitarbeitern gemeldeten False-Positives zeigen den Erfolg bei der Umsetzung der Anti-Spam-Strategie. Seinerseits muss das NOC immer wieder aktiv werden, weil fremde Rechner fälschlich die Annahme von Nachrichten aus dem Mailbackbone kategorisch ablehnen.

Birger Krägelin, zuständiger Abteilungsleiter am IITB, vergleicht die Strategie mit der Edelsteinförderung. Dort wird großflächig der gesamte Abbau abtransportiert. Erst später filtern hochempfindliche Geräte die Diamanten heraus. Der Einsatz dieser Spezialmaschinen ist unter den Bedingungen im Bergbau nicht denkbar. Übertragen auf den Mailbackbone sind die Nutzmails die Edelsteine des NOC. [Webkey 30538](#)



Foto: ITB

Einbruchversuche in die Unternehmens-IT möglichst frühzeitig zu erkennen, dabei allerdings unnötigen »Fehlalarm« zu vermeiden, ist Ziel der von »Intrusion Detection«, Systemen, die sich Methoden des maschinellen Lernens bedient. Fraunhofer-Forscher erwarten vor allem, dass sich auf diese Weise in naher Zukunft auch ein vorsorgender Schutz gegen noch völlig unbekannte Angriffsmethoden aufbauen lässt. Auch für eine automatische Überwachung und Umsetzung der Sicherheitsmechanismen im Unternehmen hat die Forschung inzwischen erste Lösungen entwickelt, wie etwa die »Information-Assurance-Architektur« des Fraunhofer IGD.

Ausfallsicherheit betrifft jeden – im Flugzeug, Aufzug oder Auto

Selbst wenn man von krimineller Energie als Risiko für den Betrieb softwarebasierter Systeme absieht, ist deren Ausfallrisiko nicht gleich Null. »Sicher« bedeutet in diesem Zusammenhang auch »betriebssicher«. So ist kaum bekannt, dass 98% aller Mikroprozessoren nicht in Desktop- oder Server-Computer eingebaut werden, sondern in die eingebetteten Systeme der unzähligen elektronischen Geräte und Systeme des Alltags. In vielen Fällen ermöglichen diese Prozessoren mit ihrer zugehörigen Software »nur« die Bereitstellung von mehr Komfort und Funktionalität, aber bei einem großen Anteil spielt Safety, also

Zutritt verboten: Um Angriffe auf die Infrastruktur möglichst frühzeitig erkennen zu können, beobachtet und analysiert das »Intrusion Detection System« den Netzwerkverkehr permanent. Auch unbekannte Angriffsmethoden zu erkennen, ist eine der großen technischen Herausforderungen.

Intelligenter Schutz vor Eindringlingen

Entwicklungstrends beim großen Bruder der »Firewall«, dem »Intrusion Detection System«

Berlin. Mit steigender Komplexität der IT-Systeme vermehren sich mögliche Schwachstellen, was von Hackern ausgenutzt werden kann. Dabei richten die Angriffe immer früher immer mehr Schaden an. Es ist daher notwendig, möglichst frühzeitig vom System gewarnt zu werden, wenn sich ein Eindringling an den Sicherheitsmechanismen des Firmennetzwerks zu schaffen macht.

„Intrusion Detection Systeme“ (IDS) analysieren riesige Mengen an Netzwerk-

verkehr und schlagen bei bekannten Angriffen beziehungsweise Anomalien Alarm. Um sich auf die ständig verändernden Angriffstechniken einstellen zu können, müssen die Systeme lernfähig sein. Auf Basis des maschinellen Lernens verbessern Wissenschaftler am Fraunhofer FIRST bestehende IDS-Taktiken im Rahmen des vom Bundesforschungsministerium geförderten Projektes MIND. Es kommen Methoden der künstlichen Intelligenz, der Statistik und dem Data Mining zum

Einsatz. Die verbesserten oder neu entwickelten Intrusion Detection Systeme sollen weniger Fehlalarme auslösen und noch unbekannte, komplexe Angriffe schnell erkennen und diagnostizieren. Damit Intrusion Detection Systeme diese Aufgabe bewältigen können, integrieren die Wissenschaftler bei FIRST sicherheitsrelevantes Expertenwissen in ihre Lernalgorithmen und entwickeln so immer intelligentere Überwachungssysteme. [Webkey 30532](#)

Betriebssicherheit, eine wesentliche Rolle. Das beginnt bei Haushaltsgeräten wie der Waschmaschine (bei der sich die Tür nur im Stillstand öffnen lassen darf) oder betrifft z.B. den Arbeitsplatz mit Aufzugs-, Roboter- und Maschinensteuerungen. Im Verkehr ist der Sicherheitsaspekt von Software offensichtlich: Heutige Verkehrsflugzeuge sind ohne das Funktionieren unzähliger Softwaresysteme überhaupt nicht mehr steuer- und navigierbar; das Cockpit wird statt von vielen Analoginstrumenten heute von zwei Multifunktionsbildschirmen dominiert. In heutigen Oberklasse-PKWs werden bis zu 100 Mikroprozessoren verbaut, auch hier die meisten für den Komfort, ein steigender Anteil jedoch für Fahrverhalten und Sicherheit.

Wenn sich Fehler nicht ausschließen lassen, kann man sie auch einplanen

Dort, wo schon kleinste Softwarefehler Menschenleben kosten können (beispielsweise im Flugzeug und in wichtigen Signalanlagen der Bahn) oder wo sich die Wartung als eher schwierig erweist (beispielsweise bei Satelliten im Orbit), fährt man immer häufiger auch eine ganz andere Strategie: Da Ausfallsicherheit nicht 100-prozentig garantiert werden kann, plant man sozusagen den Ausfall des Systems gleich von vornherein mit ein. Systeme werden doppelt oder sogar dreifach ausgelegt,



Bild: luk

Unternehmenssicherheit automatisieren

Die Umsetzung der Sicherheits-Policies darf man nicht einfach dem Zufall überlassen

Darmstadt. In Unternehmen und staatlichen Institutionen werden Sicherheitsmechanismen zum Schutz vertraulicher Informationen immer wichtiger. Doch obwohl die meisten Organisationen über umfangreiche Sicherheitsrichtlinien verfügen, werden diese häufig nur unzureichend umgesetzt. Abhilfe schafft hier die vom Fraunhofer IGD im Rahmen des Projekts COSEDA entwickelte Information-Assurance-Architektur. Mit diesem System wird die Sicherheitspolitik einer Organisation definiert und deren Umsetzung durch die integrierten »enforcing modules« automatisch durchgesetzt.

COSEDA besteht aus einer Reihe von Modulen, die jeweils auf einen bestimmten Sicherheitsaspekt ausgerichtet sind und

auch einzeln eingesetzt werden können. Drei dieser Module sind bereits einsatzbereit:

Mit TEMPROfs werden vertrauliche Informationen auf mobilen Rechnern oder externen Speichermedien geschützt, indem Dateisysteme, Verzeichnisse und einzelne Dateien automatisch und unabhängig vom Dateisystemtyp verschlüsselt werden. Außerdem wird durch einen frühzeitigen Eingriff in den Bootvorgang verhindert, dass Schlüsselmaterial beim Start ausgelesen oder Schaddateien eingespielt werden.

Das Modul Goalkeeper ermöglicht eine präzise Kontrolle von Geräteschnittstellen. Da PDAs oder Handys bislang kaum vor Angriffen Dritter geschützt sind, stellt ihre

Einbindung über Netzwerkschnittstellen eine besondere Bedrohung dar. In Goalkeeper werden Geräte, denen ein Zugriff erlaubt ist, beispielsweise anhand von Seriennummer oder Hersteller definiert. Zusätzlich werden Umgebungsmerkmale wie die Sperrung eines Arbeitsplatzes, in die Freischaltung von Geräten einbezogen.

Das Modul DMG ermöglicht einen transparenten und automatischen Schutz des E-Mail-Verkehrs. Die Verschlüsselung der E-Mails wird erzwungen und kann weder umgangen werden noch belastet sie den Nutzer. Außerdem werden sensible Inhalte auch bei durch VPN- oder SSL/TLS geschützten Mails erkannt und dann selbsttätig blockiert oder verschlüsselt.

und zwar so, dass ein System innerhalb von Sekundenbruchteilen die Aufgaben des anderen übernehmen kann. Da Hard- und Software in solchen Fällen meist eigens entwickelt werden müssen und nachträgliche Anpassungen sehr schwierig sind, verursachen diese redundanten Systeme vergleichsweise hohe Entwicklungskosten. Diese Kosten lassen sich mit »everControl«, einer Entwicklung am Fraunhofer FIRST, deutlich reduzieren. Außerdem ist eine Zertifizierung schneller zu erreichen als sonst. Jedes der drei Steuerungsmodulare ist mit einem eigenen Echtzeitbetriebssystem ausgestattet, das nach einem Absturz in Sekundenschnelle wieder läuft.

Darf Sicherheit auch auf Kosten der Funktionalität gehen?

Erschwert wird die konsequente Umsetzung von Safety vor allem durch die wirtschaftlichen Rahmenbedingungen. So ist im Gegensatz zur Luft- und Raumfahrt eine Funktionseinschränkung zugunsten von mehr Sicherheit in Massenartikeln schwer zu vermitteln. Auch der hohe Kostendruck z.B. auf dem Automobilsektor erlaubt es oft nicht, hoch zuverlässige Bauteile einzusetzen oder Systeme sicherheitshalber mehrfach auszulegen. Hier sind intelligente Ansätze gefragt, um die Geschäftsziele mit möglichst wenigen Kompromissen hinsichtlich der Betriebssicher-



Europas Taskforce für IT-Sicherheit

Forscher bündeln ihre Anstrengungen, um länderübergreifende Strategien zu entwickeln

St. Augustin. Der größte Stromausfall Amerikas oder die unfreiwillige Stilllegung des Londoner Flughafens Heathrow haben gezeigt, wie stark Informations- und Kommunikationstechnologien sämtliche Infrastrukturen in Wirtschaft und Gesellschaft durchdrungen haben. Um die Sicherheit kritischer Infrastrukturen zu verbessern, hat die Europäische Union das Projekt »CI²RCO« (Critical Information Infrastructure Research Coordination) gestartet, das entsprechende Forschungen bündeln soll.

»Ziel des Projekts ist die Bildung einer europäischen Taskforce, die Forschung und Entwicklung zum Schutz kritischer Informationsstrukturen fördert und koordiniert«, sagt Paul Frießem vom Fraunhofer SIT. »Europa hat die Notwendigkeit zu solch konzertierten Bemühungen später erkannt als etwa die Vereinigten Staaten oder Kanada. Jetzt liegt es an uns Europäern, diesen Rückstand aufzuholen und länderübergreifende Strategien und Konzepte zu entwickeln.«

An dem Projekt, das bis 2007 laufen wird, sind neben dem Fraunhofer-Institut auch das Deutsche Zentrum für Luft- und Raumfahrt, die Industrieanlagen-Betriebsgesellschaft mbH, die Firma Ernst Basler+Partner aus der Schweiz, die italienische ENEA, die französische Groupe des École des Télécommunications – École Nationale Supérieure des Télécommunications sowie die niederländische Organisation für angewandte Wissenschaften (TNO) beteiligt. [Webkey 30539](#)



IT-Unternehmen verlangen Antworten von der Politik

BITKOM fordert eine bessere Abstimmung zwischen Bund und Ländern

Deutsche IT-Unternehmen sehen im Thema »Homeland Security« eine der größten Herausforderungen.

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) hat hierzu eine

Projektgruppe ins Leben gerufen. Im Interview: **Fabian Bahr, Bereichsleiter Wirtschafts- und Innovationspolitik beim BITKOM.**

Im Bereich Sicherheit verschmelzen ziviler und militärischer Bereich immer stärker miteinander. Löst sich auch in der deutschen ITK-Wirtschaft die Grenze zwischen innerer und äußerer Sicherheit auf?

Bahr: Deutschlands Sicherheit macht längst nicht mehr an den Grenzen Halt. Es sollte jedem klar sein, dass die Entwicklung der letzten Jahre zu einem neuen Verständnis von »äußerer Sicherheit« geführt hat, nämlich dass diese Sicherheit eben nicht nur in Deutschland und Europa verteidigt werden muss. Die neue Dimension, die durch potentielle Bedrohungen der inneren Sicherheit entsteht – nehmen Sie nur den internationalen Terrorismus oder großflächige Katastrophenlagen – sind politisch teils unzureichend perzipiert und umgesetzt worden. »Homeland Security« kann sich somit nicht auf die Themenfelder innere und äußere Sicherheit beschränken. Er ist vielmehr der neue Oberbegriff aller öffentlichen und privatwirtschaftlichen Aufgabenfelder, die der Wahrung der inneren und äußeren Sicherheit dienen. Die wechselnden Anforderungen, die aus derart dynamischen Bedrohungslagen hervorgehen, können folgerichtig nur in einem allumfassenden, übergreifenden Ansatz zusammengefasst werden.

Wie stehen denn aus Sicht des BITKOM die politischen Vorzeichen für einen solchen ganzheitlichen Ansatz?

Bahr: Das Fehlen einer zwischen Bund und Ländern abgestimmten Strategie, eines einheitlichen Ansprechpartners sowie die Themenzersplitterung auf dem Gebiet »Homeland Security« sind nur einige in der Projektgruppe HLS des BITKOM kritisch

diskutierte Punkte. Diese Probleme drängen sich um so mehr auf, als nicht nur der Public Sector, sondern potenziell auch Branchen wie Logistik, Chemie oder auch Infrastrukturbetreiber (beispielsweise Wasser- und Energieversorgung) aufgefordert sind, sich mit dem Thema auseinanderzusetzen. Die Herausforderungen, vor denen Deutschland in diesem Zusammenhang steht, sind jedenfalls beachtlich.

Welche konkreten Weichenstellungen fordern Sie also von der Politik? Und welche Rolle hat aus Ihrer Sicht hierbei die Forschung?

Bahr: Für mehr »vernetzte Sicherheit« ist die Politik insbesondere gefordert, Konzepte für eine gesamtstaatliche Sicherheitsarchitektur zu entwickeln und diese mit einem Umsetzungsplan und den entsprechenden finanziellen Mitteln zu verbinden. Außerdem müssten ein koordinierender Ansprechpartner für »Homeland Security« benannt sowie Kooperationsmodi für Behörden und Dienste in Deutschland über Landesgrenzen hinweg gefunden werden. Beim Einsatz neuer Technologien sollten Standardisierung und Interoperabilität stärker berücksichtigt werden. Und nicht zuletzt muss dringend die Zusammenarbeit zwischen Wirtschaft und Forschungseinrichtungen stärker öffentlich gefördert werden, damit Unternehmen auch auf die langjährige Expertise der Wissenschaftler zurückzugreifen können.



Fabian Bahr

Welchen Beitrag können denn Sicherheits-Technologien aus Deutschland zur Sicherung des Wirtschaftswachstums leisten?

Bahr: Das technologische Potenzial ist hervorragend: Katastrophenschutz, Biometrie, kritische Infrastrukturen – sie alle haben Informations- und Kommunikationstechnologien als Kernbestandteil gemeinsam. Über Informationsgewinnung, -verarbeitung, -übermittlung und -verwendung hinweg ist der Einsatz von Informations- und Kommunikationstechnologien zur grundlegenden Bedingung für die Umsetzbarkeit von Sicherheitsstrategien geworden. Kein gemeinsames Lagebild, keine behördenübergreifende Kommunikation, keine Schutzmaßnahmen gegen den internationalen Terrorismus oder gegen die organisierte Kriminalität können ohne modernste Informations- und Kommunikationstechnik umgesetzt werden.

Welche Notwendigkeit und welches Potenzial sehen Sie in einer verstärkten Zusammenarbeit von angewandter ITK-Forschung und Ihren Mitgliedern?

Bahr: Politik und Verwaltung, Wirtschaft, Wissenschaft und Gesellschaft sind gemeinsam gefordert, in einem partnerschaftlichen Ansatz zur Lösung der branchen- und ressortübergreifenden Aufgaben beizutragen. Die neue Projektgruppe »Homeland Security« des BITKOM versteht sich genau hierfür als Plattform. Daneben bestehen zwischen unserem Verband und der Fraunhofer-Gruppe enge Kontakte auf verschiedenen Ebenen.

Fragen: Alexander Gerber-Crawford

heit zu erreichen. Dabei darf man sicherheitskritische eingebettete Systeme nicht nur als Sicherheitsrisiko betrachten; im Gegenteil: Viele heutige Sicherheitsfeatures werden durch elektronische Systeme erst ermöglicht. Ein Beispiel ist das verbreitete ABS; weiter entwickelte Systeme wie ESP, ASR oder Bremsassistenten werden erst nach und nach zum Standard in allen Fahrzeugklassen. Dass sich Fahrzeuge über Funksignale gegenseitig bei Gefahrensituationen warnen und Bremsmanöver vorbereiten, ist bereits in Vorbereitung.

Sicherheit wird zunehmend ein Thema für eingebettete Systeme

Dieser steigende Anteil (betriebs-)sicherheitskritischer Anwendungen von Software muss seinen Niederschlag im Software-Engineering finden. Insbesondere im Bereich der Eingebetteten Systeme, wo die erforderliche Software teilweise noch von Hardware-Fachingenieuren ohne spezielle Softwaretechnik-Ausbildung entwickelt wird, besteht großer Nachholbedarf. Sicherheit im Sinne von Betriebssicherheit ist auch hier nicht nachträglich in ein Produkt einzubauen – dieser Aspekt muss schon in der Anforderungsphase berücksichtigt und dann kontinuierlich verfolgt werden.

Bei allen Bemühungen, softwarebasierte Systeme möglichst sicher im Bezug auf Security und Safety zu gestalten, wird man Fehler im Sinne von (erfolgreichen) Angriffen oder Ausfällen selten ganz verhindern können. Neben einer raschen Behebung der Ursachen ist auch die genaue Analyse des Vorfalls von Bedeutung, um die gewonnenen Erfahrungen zur Bearbeitung vergleichbarer **Störfälle** heranziehen zu können. Genau dies leistet ein erfahrungsbasierter Störfall-Leitstand, der sich

Im Ernstfall trotzdem die Kontrolle behalten

Viele Probleme werden beherrschbar, wenn auch die Software lernt, aus Fehlern zu lernen

Kaiserslautern. Die schnell wachsende Abhängigkeit heutiger Geschäftsabläufe von Informations- und Kommunikationstechnologien erfordert, dass Störungen minimiert und im Falle des Eintretens zügig behoben werden. Kommt es beispielsweise während des Imports von Buchungssätzen in das zentrale System des Finanzwesens zum Systemabsturz, stellen sich sofort eine ganze Reihe von Fragen: Wie lässt sich nun vermeiden, dass Dubletten von Buchungssätzen erzeugt oder aber ganze Buchungssätze verloren gehen? Der Service-Mitarbeiter verlässt sich in einem solchen Fall normalerweise auf Systemliteratur oder auf seine persönlichen Erfahrungen, oder er vertraut auf den Rat von KollegInnen mit entsprechenden Kenntnissen und Erfahrungen. Diese Reaktion

mag zwar nahe liegen, ist aber in verschiedener Hinsicht unzulänglich: Weder das persönliche Erfahrungswissen noch das einzelner KollegInnen kann allzeit aktuell und umfassend sein. Eine zentrale Speicherung, Pflege und Verknüpfung von Erfahrungswissen findet nicht statt. Zudem erfordert die Informationsrecherche eine Arbeitsunterbrechung und verzögert damit die Reaktion auf die Störung.

Erfahrungen der Mitarbeiter nutzen

Die optimale Lösung ist in der Regel ein systematisches IT-Störfall-Management, das individuelle Erfahrungen in einer Organisation allgemein zugänglich macht und diese innerhalb des Arbeitsprozesses direkt zur Verfügung stellt – ein besonderer Vorteil nicht nur bei großen

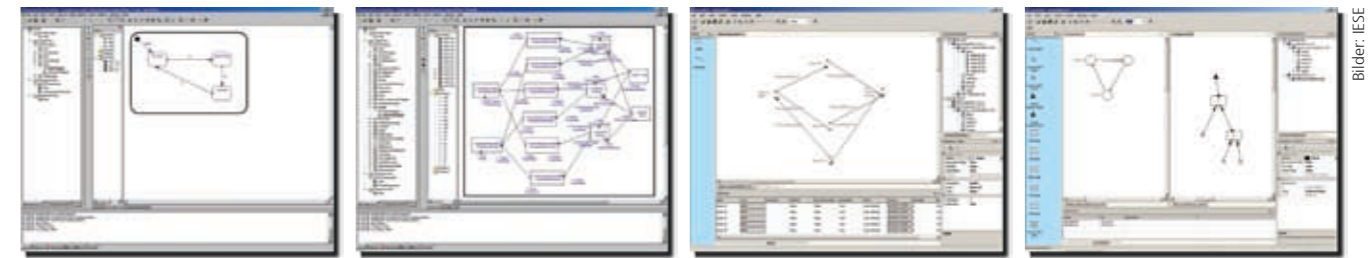
Teams, wechselnden Zuständigkeiten und hoher Personalfuktuation. Konventionelle Trouble-Ticket-Systeme, die häufig im Supportbereich für die Erfassung von Störungen eingesetzt werden, genügen diesen Anforderungen nicht. Sie tragen zwar den organisatorischen Aspekten Rechnung, lassen jedoch das Erfahrungswissen der Mitarbeiter ungenutzt.

Genau hier setzt der »IT-Störfall-Leitstand« des Fraunhofer IESE an: Damit wird der IT-Support-Prozess unter allen inhaltlichen und organisatorischen Gesichtspunkten gleichermaßen unterstützt; Erfahrungswissen wird automatisch erfasst und situationsspezifisch zur Verfügung gestellt.

Das erfahrungsbasierte IT-Störfallmanagement des Fraunhofer IESE basiert auf zwei wesentlichen Aspekten: Ein einfacher

Safety by Design – Betriebssicherheit als Entwicklungskonzept

Neue Werkzeuge unterstützen Software-Ingenieure bei der Entwicklung technischer Systeme



Bilder: IESE

Kaiserslautern. Technik, die durch Software gesteuert wird, ist nur dann wirklich »betriebsicher«, wenn der gesamte Entwicklungsprozess durchgängig auf Sicherheit ausgerichtet wird. Sicherheit lässt sich nicht nachrüsten und kann oft auch nicht allein der Software eines Systems zugeschrieben werden.

Der Entwicklungsprozess betrifft also das Gesamtsystem. Je nach Sicherheitsbedarf sind die Ansprüche an die Verfahrensweisen und die verwendeten Techniken dabei unterschiedlich hoch. Schon bei der Produktdefinition werden Risiken

und Gefahren identifiziert und zu deren Vermeidung oder Erkennung Sicherheitsanforderungen an das Produkt definiert. Hier kommen zum Beispiel Techniken wie die Fehlerbaumanalyse, die Failure Modes and Effects Analysis (FMEA) oder die Ereignisbaumanalyse zum Einsatz.

Die Sicherheitsanstrengungen reichen über alle Phasen des Entwicklungsprozesses bis in die Betriebsphase des Systems, wo alle Prozeduren für Wartung, Fehlerkorrektur und Änderungen genau definiert und dokumentiert sind. Sicherheit wird also durch ein ganzes Bündel von konstruktiven und

analytischen Techniken und Maßnahmen erreicht, die ein hohes Maß an Expertise und eine durchgängige Werkzeugunterstützung erfordern. Hier laufen in der Fraunhofer-IuK-Gruppe vielfältige Forschungsaktivitäten. Ein Beispiel ist das Werkzeug »ESSaRel«, das über die Website des Fraunhofer IESE kostenlos zur Evaluation heruntergeladen werden kann. Es vereint eine für Software-Aspekte erweiterte Fehlerbaumanalyse mit zustandsbasierten Modellen und bietet obendrein den Import von Software-Modellen aus gängigen CASE-Tools an.

Workflow mit »To-Do-Listen« unterstützt einerseits den organisatorischen Ablauf des Betriebs und der Wartung. Eine Erfahrungsdatenbank, die in diesen Workflow integriert ist, bietet andererseits intelligente Unterstützung bei Störfällen und Ausnahmesituationen. Diese beruht auf praxiserprobten Methoden des Fallbasierten Schließens (Case-Based-Reasoning) sowie auf Information-Retrieval-Verfahren, die unaufdringlich in den Arbeitsprozess integriert sind. Suchanfragen werden aus dem aktuellen Arbeitskontext heraus automatisch erzeugt – damit lässt sich eine solche »intelligente Hilfsfunktion« deutlich einfacher anwenden als herkömmliche wissensbasierte Systeme ohne Integration in den Arbeitsprozess. In der täglichen Praxis des Störfallmanagements werden alle

relevanten Phasen durch den IT-Störfall-Leitstand unterstützt:

Statusüberwachung: Jeder Vorfall wird automatisch entdeckt oder gemeldet und in den Leitstand eingetragen. Jedem Vorfall wird dabei ein Mitarbeiter zugeordnet.

Diagnose, Entscheidung, Reaktion: Vorschläge von Problemlösungswegen, alternativen Ursachen, Ansprechpartnern und so weiter bieten eine intelligente Entscheidungsunterstützung. Während der Bearbeitung des Vorfalls werden Arbeitsstatus und Abweichungen gegenüber den Vorschlägen protokolliert, wodurch der aktuelle Arbeitsstatus stets für Mitarbeiter und IT-Manager abrufbar ist. Der eingeschlagene Lösungsweg wird analysiert und

die Erfahrungsdatenbank entsprechend ergänzt. Auf diese Weise lernt der IT-Störfall-Leitstand aus der täglichen Praxis – automatisch im Hintergrund, ohne Mehraufwand für die Benutzer. Jenseits des Routinebetriebs unterstützt der IT-Störfall-Leitstand einen kontinuierlichen

Verbesserungsprozess: Die systematische Erfassung von Vorfällen und Reaktionen bietet die Grundlage für Verbesserungsmaßnahmen. Diese können sowohl organisatorischer als auch technischer Natur sein. Beispielsweise wird durch Analysen der Erfahrungen erkannt, wo eine Automatisierung vorteilhaft ist. Außerdem bietet das System Hilfestellung bei der Anpassung der Lösungswege im Falle von Änderungen an der Software.

zudem unauffällig in den laufenden Betrieb integriert und die Mitarbeiter nicht mit zusätzlichen Verwaltungsarbeiten belastet. Auch Analysewerkzeuge zur Vorhersage des Sicherheitsverhaltens einer Software anhand von Modellen schon während der Software-Entwicklung sind mittlerweile unverzichtbar. Basis für die sinnvolle Anwendung jeglicher Werkzeuge und Techniken ist jedoch ein ausgereifter Software-Entwicklungsprozess und damit die praktische Anwendung ingenieurmäßiger Verfahren. Sollte einmal doch der Ernstfall eintreten und nur noch Schadensbegrenzung angesagt sein, ist zumindest ein professionelles **IT-Incident-Management** erforderlich. Auch auf solche »Ernstfälle« kann und muss sich ein Unternehmen vorbereiten.



Computerkriminellen auf der Spur

Was wäre wenn: Vorbereitungen auf den Ernstfall verlangen nach IT-Incident Management

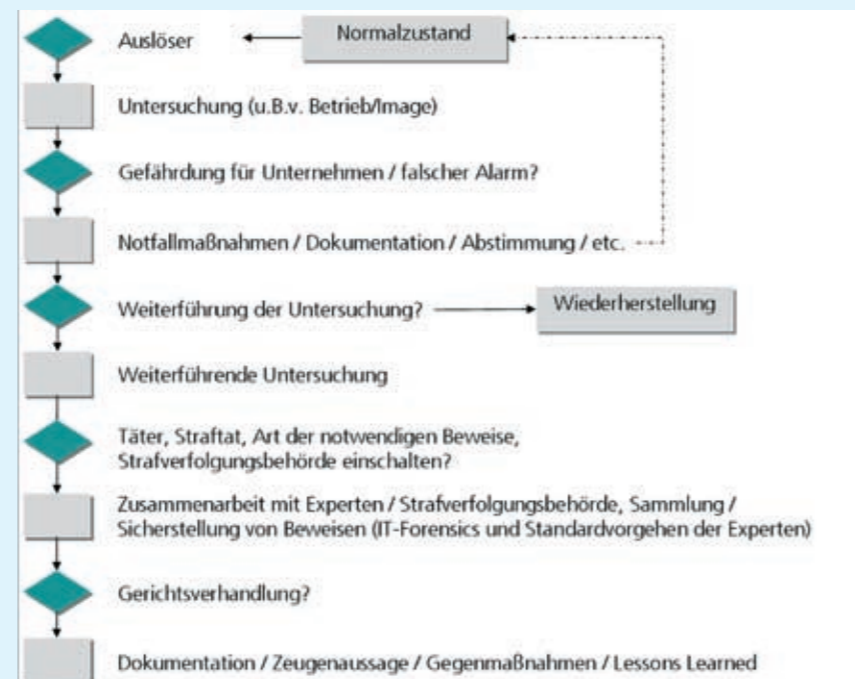
Stuttgart. Die gerade veröffentlichte Kriminalstatistik des Bundeskriminalamtes für 2004 spricht von fast 67.000 der Polizei gemeldeten strafrechtlichen Sachverhalten im Umfeld der »Computerkriminalität« – ein Anstieg von gut 12 Prozent gegenüber 2003. Da auf der einen Seite der Begriff Computerkriminalität einen großen, nicht eindeutig definierten Bereich abdeckt und zusätzlich (oder gerade deswegen?) diese Straftaten leicht unentdeckt bleiben können, ist von einer sehr hohen Dunkelziffer auszugehen.

Spuren am »Tatort Computer«

Ein Unternehmen muss sich also nicht nur vor kriminellen Handlungen schützen, sondern sich ebenso auf den Ernstfall vorbereiten. Mehrere Institute der Fraunhofer-IuK-Gruppe erforschen deshalb nicht nur die Prävention, sondern auch das Aufspüren und Ermitteln solcher Vergehen. Um hierbei strukturiert handeln zu können, sind standardisierte Vorgehensweisen nötig, die einen ganzheitlichen Ansatz verfolgen, wie etwa ein IT-Incident-Management.

Die Vorbereitung auf den Ernstfall besteht aus mehreren Phasen: Planung, Betrieb, Ermittlung (IT-Forensik) und Nachbereitung. Prozesse sind aus technischer, organisatorischer und rechtlicher Sicht so zu gestalten und zu etablieren, dass alle Beteiligten ihre

Verantwortungsbereiche und Aufgaben genau kennen, sie verstehen, und – wichtiger noch – dafür qualifiziert sind und sie leben. Somit ist Sensibilisierung ein kleiner aber wichtiger Erfolgsfaktor gegen Computerkriminalität. [Webkey 30526](#)



Sichere Großstädte

St. Augustin. Ein fundierter Erfahrungsaustausch zwischen europäischen Großstädten über Ideen und Konzepte zu Krisenvorbeugung und -management ist Ziel des im Frühjahr gestarteten Projektes »Security and Trust in Cities« (SETRIC). Auf gemeinsamen Workshops und Konferenzen, wie jüngst beim Auftaktkongress im Fraunhofer FIT, sollen europaweite Richtlinien erarbeitet sowie Lücken zwischen Forschung und Praxis geschlossen werden.

Sicherer Finanzmarkt

Darmstadt. Besonders Banken und Versicherungen müssen ihre Kunden beim elektronischen Geschäftsverkehr wirksam schützen, da sie auf deren Vertrauen angewiesen sind. Ein Security-Seminar speziell für Entscheider aus dem Finanzmarkt informierte in Frankfurt über den technischen und organisatorischen Schutz vor IT-Risiken. Veranstaltet wurde das Seminar vom Fraunhofer SIT in Kooperation mit SUN, ISS und der danet Group. Themen waren unter anderem Risikomanagement, Angriffsschutz und Identity Management. [Webkey 30524](#)

Neue Middleware für sichere RFID

Darmstadt. Auch RFID-Systeme enthalten oft Informationen, die nicht in falsche Hände geraten dürfen. Daher hat das Fraunhofer SIT die herstellerneutrale RFID-Middleware »SAN« entwickelt und jetzt auf der »Sensor« in Nürnberg präsentiert. »SAN« schützt Unternehmen vor Datenverlust, Systemstörungen und Spionage. Das ist vor allem dann wichtig, wenn RFID über Unternehmensgrenzen hinweg eingesetzt wird, wie etwa in der Logistik. [Webkey 30521](#)

Digitale Signatur ohne Verfallsdatum

Darmstadt/Hannover. Damit elektronisch signierte Dokumente archiviert werden können, müssen die Signaturen in regelmäßigen Abständen mit Zeitstempeln erneuert werden. Um kostspielige Zeitstempel für jedes Dokument zu vermeiden, hat das Fraunhofer SIT mit dem Programmpaket »ArchiSoft« eine Lösung entwickelt, bei der nur ein Zeitstempel für mehrere Dokumente benötigt wird: Dabei werden die Dokumente als Baum angeordnet und in Richtung der Wurzel sukzessive kryptografische Quersummen, sogenannte Hashwerte, gebildet. Dadurch erhält man einen einzigen Hashwert für den gesamten Baum und alle darin enthaltenen Dokumente und braucht nur dafür einen Zeitstempel. »ArchiSoft« ist ein Ergebnis des Projekts »ArchiSig«. Daran knüpft das Folgeprojekt »TransiDoc« an, das für die rechtssichere Dokumententransformation in Kommunalverwaltung, Gesundheitswesen und Notariaten Konzepte und Lösungen entwickelt. [Webkey 30519](#)

Biometrieplattform

Berlin. Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) begrüßt die zügige Einführung eines neuen Reisepasses mit biometrischen Sicherheitsmerkmalen. Um darüber hinaus die Entwicklung moderner Sicherheitstechnologien in Deutschland weiter voranzutreiben, schlägt der BITKOM die Gründung einer nationalen Biometrie-Initiative vor, die Politiker, Vertreter der Industrie, Wissenschaftler und Anwender an einen Tisch bringen soll. Die Teilnehmer können technische Fragen der Standardisierung besprechen, Referenzprojekte anstoßen und rechtliche Themen diskutieren. [Webkey 30517](#)

Deutsch-japanisches Sicherheits-Symposium

Tokio. Der »Münchner Kreis« organisiert unter Beteiligung des Fraunhofer SIT vom 13. bis 16. September ein deutsch-japanisches Symposium zum Thema »Security, Privacy and Safety in the Information Society«. Ziel ist der bilaterale Austausch über aktuelle Herausforderungen und Lösungen für die IT-Sicherheit. Zur Eröffnung spricht Prof. Claudia Eckert, Institutsleiterin am SIT, über »Trends and Challenges in Security, Privacy and Safety«. Der Themenblock »Vulnerability and Protection of the Information Society« beschäftigt sich mit nationalen Strategien zum Schutz kritischer IT-Infrastrukturen sowie mit Vorsorgemaßnahmen in Unternehmen. Sicherheitslösungen für eine Vielfalt von unterschiedlichen Geräten, Netzen und Plattformen, dabei besonders auch von mobilen Geräten, werden im Themenbereich »Security in Ubiquitous Systems and Applications« diskutiert. Um das Sicherheitsrisiko durch menschliche Benutzer zu reduzieren, werden im Themenblock »Social Impacts and Challenges, Security Education and Awareness« Lösungen zur gezielten Schulung des Personals besprochen. Damit nur autorisierte Benutzer Zugriff bekommen, werden im Block »Digital Rights Management and Information Rights Management« biometrische Zugangskontrollen, DRM-Systeme und Lösungen zur Dokumentensicherheit vorgestellt. In jedem Themenblock findet nach dem Vortrag von Experten beider Länder eine Podiumsdiskussion statt. Das Symposium wird ergänzt durch eine deutsch-japanische Fachausstellung. Vorsitzender des Programmausschusses auf deutscher Seite ist Prof. Heinz Thielmann, bis 2004 Leiter des Fraunhofer SIT. [Webkey 30517](#)

Geodaten einfach übers Internet

Darmstadt. Geodaten wie Grundstücksbeschreibungen oder Karten, die die Nutzer einfach über das Internet abrufen können – damit bietet ALKIS®, das »Amtliche Liegenschaftskataster-Informationssystem«, jetzt einen neuen Service. Über die technischen Grundlagen des Systems informierte der vom Zentrum für Graphische Datenverarbeitung veranstaltete Kongress »XML und ALKIS®«. Da ALKIS® eine auf XML (eXtended Markup Language) basierende Schnittstelle verwendet, können die Informationen mit jedem Browser angezeigt werden. Weitere Themen des Kongresses waren die Möglichkeit, Fachinformationssysteme an ALKIS® anzubinden, sowie Struktur und Modellierungsmöglichkeiten der »Geography Markup Language« GML3. Außerdem wurden die Impulse für die Geoinformationswirtschaft erläutert. [Webkey 30505](#)

IT-Lösungen gegen ein olympisches Babylon

Darmstadt. Millionen Besucher und Zehntausende Sportler aus aller Welt machen die Olympischen Spiele 2008 in Peking zu einer informationstechnischen Herausforderung. Da nur die Wenigsten Chinesisch verstehen, müssen alle wichtigen Informationen in der Stadt mehrsprachig verfügbar sein. Im Rahmen des Projekts »Compass 2008« arbeitet das Fraunhofer ISST zusammen mit dem Institute of Computing Technology (ICT) in Peking an einer Plattform für individuelle und mehrsprachige Informationsdienste. Die Benutzer sollen damit die für sie relevante Informationen ortsabhängig in ihrer jeweiligen Sprache im Internet oder auf mobilen Geräten abrufen können. [Webkey 30513](#)

E-Learning auch für das Handwerk

Stuttgart. Um kleine Unternehmen und insbesondere Handwerksbetriebe dabei zu unterstützen, die für sie richten E-Learning-Lösungen zu finden, wird im Rahmen des EU-Projekts »eLISHE« (E-Learning Inventory for Small and Handcraft Enterprises) eine Internetpräsenz erstellt, die über existierende Produkte und laufende Projekte informiert. In dem Projekt kooperieren Experten aus sechs EU-Ländern, der deutsche Vertreter ist das Institut für Arbeitswirtschaft und Technologiemanagement (IAT) der Universität Stuttgart, das eng mit dem Fraunhofer IAO kooperiert. Die Projektpartner dokumentieren das aktuelle Angebot, untersuchen aber auch die Anforderungen an Produkte und derzeitige Mängel, damit in den folgenden Jahren die Entwicklung entsprechend angepasst wird. [Webkey 30507](#)

ÖPNV als moderner Dienstleister

Darmstadt. Lang ist die Liste der Anforderungen an die Dienstleistungsbetriebe im Öffentlichen Personennahverkehr (ÖPNV). Kunden erwarten heutzutage mehr als nur den Transport von A nach B. Schnell und unkompliziert möchten sie sich über die beste Verbindung, Anschlussmöglichkeiten und die Preise informieren können. Das Fraunhofer IGD präsentierte auf dem »Traffic Day« verschiedene Lösungen: Beispielsweise haben die Forscher Konzepte entwickelt, um Wegbeschreibungen auf mobilen Geräten, wie PDA oder Handy, dreidimensional darzustellen. Denn Studien haben ergeben, dass die meisten Menschen 3D-Karten besser lesen können.

Integrierte Ambient-Intelligence-Lösungen

Kaiserslautern. Geräte in Büro und Alltag übernehmen eigenständig immer mehr Routine-Funktionen und fangen an »mitzudenken«. Doch für eine wirklich intuitiv bedienbare, allgegenwärtige elektronische Assistenz (»Ambient Intelligence«) sind noch etliche Fragen offen, beispielsweise, wie die Geräte und Systeme untereinander kompatibel, nahtlos und vor allem sicher kommunizieren können. Unter Federführung der IuK-Gruppe bündeln die Fraunhofer-Institute deshalb jetzt ihre Entwicklungen auf diesem Gebiet. Auf einem gemeinsamen Workshop wurden die existierenden Lösungen und Kompetenzen analysiert und Konzepte entwickelt, wie sie sich zu funktionierenden und demonstrierbaren Gesamtszenarien kombinieren lassen. Anhand dieser integrierten Lösungen wird sich das Potenzial von Ambient Intelligence in den verschiedenen Anwendungsbe-reichen anschaulich darstellen lassen.

Hier ist der Kunde noch König

Stuttgart. Zum dritten Mal haben das Fraunhofer IAO, das Wiesbadener Unternehmen Mewa Textil-Service AG & Co. und das Magazin »impulse« den »Deutschen Service-Preis« vergeben. Rund 140 Unternehmen bewarben sich mit praxiserprobten Service-Konzepten um die mit insgesamt 20.000 Euro dotierten Preise. Der erste Platz und 10.000 Euro gingen an das Bremer Unternehmen »SUS Senioren-Umzugs-Service« von Karen Pretzer. Sie organisiert für Senioren alle mit dem Umzug verbundenen Aufgaben. Auch in diesem Jahr können sich innovative Dienstleister wieder um den Deutschen Servicepreis bewerben. [Webkey 30515](#)

Relativitätstheorie in 3D veranschaulichen

Berlin. Mit dreidimensionalen, virtuellen Darstellungen anstelle von komplizierten Erklärungen veranschaulichte die von Fraunhofer FIRST entwickelte digitale Litfaßsäule auf dem Berliner Wissenschaftssommer Einsteins Relativitätstheorie. Abends wurde die Litfaßsäule in die Cross-Media Kurzoper »C - The Speed of Light« eingebunden. Für die dreidimensionale Darstellung sind im Inneren der Litfaßsäule acht Projektoren angebracht, die die vier Bildteile in Stereoprojektion ausleuchten. Die 3D-Brille des Betrachters enthält das Trackingsystem, das seine Position bestimmt und daran die Bilddarstellung anpasst – ein Bildeindruck wie ein Hologramm, das im Inneren der Säule schwebt und von allen Seiten betrachtet werden kann. [Webkey 30509](#)

Vernetztes Arbeiten in China und Indien

Stuttgart. Das Fraunhofer IAO veranstaltet vom 23.- 30. Oktober 2005 eine Studienreise nach China und Indien. Besucht werden Shanghai sowie Mumbai, Pune und Bangalore. Innerhalb einer Woche lernen die Teilnehmer zwei der wirtschaftlich am schnellsten wachsenden Regionen dieser Erde intensiv kennen. Im direkten Austausch mit deutschen Managern und Vertretern lokaler Unternehmen entwickeln die Teilnehmer Lösungsmodelle für das vernetzte und verteilte Arbeiten. Im Vordergrund stehen Fragestellungen zu infrastrukturellen Voraussetzungen, Kostenstrukturen, Arbeitszeitmodellen und Schlüsselqualifikationen. Um einen intensiven Austausch und Wissenstransfer sicherzustellen, ist die Teilnehmerzahl auf 15 Personen beschränkt. Weitere Informationen sind über den Webkey erhältlich. [Webkey 30514](#)

3D für zwei auf den Punkt gebracht

St. Augustin. Auf einer Virtual-Reality-Tagung mit der Öl- und Gasindustrie präsentierte das Fraunhofer IMK jetzt ein System, mit dem zwei Benutzer gleichzeitig mit virtuellen Objekten interagieren können. »TwoView« ermöglicht so beispielsweise die gemeinsame Analyse komplexer Daten oder das kollaborative Engineering. Dabei erzeugt »TwoView« für jeden der beiden Benutzer ein eigenes stereoskopisches 3D-Bild. Bei anderen 3D-Systemen hängt die Position des Objekts dagegen von der Position des Betrachters ab und es ergibt sich für jeden Benutzer eine andere räumliche Darstellung. [Webkey 30506](#)

Ehrenprofessur für russische Kooperation

Erlangen/Wladimir. Prof. Heinz Gerhäuser, Leiter des Fraunhofer IIS, sowie Prof. Heinrich Niemann, Lehrstuhl für Mustererkennung der Universität Erlangen-Nürnberg, haben eine Ehrenprofessur der russischen Staatlichen Universität Wladimir erhalten. Den Titel erhielten sie für ein Programm, das russischen Studierenden ermöglicht, in Erlangen Praktika zu absolvieren, deren Ergebnisse in russische Hochschulabschlüsse einfließen. [Webkey 30508](#)

Offene Institute

Darmstadt. Im Rahmen der »Woche der Wissenschaft« präsentierten sich auch die drei Darmstädter Fraunhofer-Institute der Öffentlichkeit: Institutsführungen vermittelten den Teilnehmern einen Einblick in die Forschung, beispielsweise digitale Wasserzeichen bei einer »Straßen-Vorlesung« und Sicherheitslücken bei der Bluetooth-Technologie.

Lebenslanges Lernen für die Arbeitswelt

Stuttgart. Wer die eWorld-Ausstellung auf der CeBIT 2005 verpasst hat oder wer sie gesehen hat und nun mehr wissen will, kann auf das im März erschienene Buch »e3World« zurückgreifen. Dieter Spath, Institutsleiter des Fraunhofer IAO, Walter Ganz und Till Becker thematisieren darin das Konzept des lebenslangen Lernens in der Arbeitswelt. Das Buch gliedert sich in drei Bereiche: im Teil »work« geht es um den Wandel der Arbeitswelt an sich, der Teil »learning« befasst sich mit den erforderlichen Qualifizierungsmaßnahmen, um diesen Wandel zu bewältigen, und im Teil »performance« stehen die Unternehmensprozesse und deren Performanz im Vordergrund. Denn ob Weiterbildungsmaßnahmen finanziert werden, hängt meistens von messbaren Erfolgskriterien ab. [Webkey 30516](#)

Fahrassistenzsysteme im Praxistest

Stuttgart. Wie müssen Fahrassistenzsysteme beschaffen sein, um tatsächlich ihren Zweck zu erfüllen? Das untersuchen das Fraunhofer IAO und das Institut für Arbeitswissenschaft und Technologiemanagement (IAT) der Universität Stuttgart im Rahmen des EU-Projekts »AIDE«. Damit die Sensoren und Anzeigen vom Fahrer akzeptiert werden, müssen sie genau auf die Verkehrssituation und den Fahrstil abgestimmt sein. Drei Demonstrationsfahrzeuge dienen zum Testen dieser individuellen Anpassung. Außerdem werden für eine Begleitstudie noch Probanden aus Stuttgart und Umgebung gesucht, die Fahrassistenzsysteme nutzen oder demnächst nutzen werden. [Webkey 30510](#)

Fachtagung zum Thema lernende Maschinen

St. Augustin. Die weltweit größte internationale Fachtagung für maschinelles Lernen, die ICML (International Conference on Machine Learning) wird in diesem Sommer an der Universität Bonn vom 7. - 11. August 2005 stattfinden. Zahlreiche Wissenschaftler von Weltrang, darunter Nobelpreisträger, und Experten von Daimler Chrysler, Google, Yahoo, Siemens, Microsoft, IBM, NASA und viele mehr werden auf der Tagung des Fraunhofer AIS über neueste Forschungsergebnisse und Anwendungen in den Bereichen maschinelles Lernen, Data Mining und intelligente Wissensextraktion sprechen. Als zentrales wissenschaftliches und zunehmend auch anwendungsorientiertes Forum für ein Kerngebiet der Künstlichen Intelligenz findet die Konferenz nach sechs Jahren erstmals wieder in Europa statt – erstmals in Deutschland. [Webkey 30512](#)

Surround-Sound über das Radio

Erlangen/München. Wie Surround-Klang über Radio und ohne aufwändige Lautsprechersysteme möglich ist, demonstrierte das Fraunhofer IIS jetzt gleich zweimal: Auf der NAB in Las Vegas lief im Digitalradio die erste Rundfunksendung in echtem 5.1-Surround-Sound, die live über ein entsprechend erweitertes Autoradio dekodiert wurde. Um Klangdateien mit Surround-Sound zu versehen, kodiert die Spatial Audio Software vom Fraunhofer IIS die Daten platzsparend als Stereosignal mit Zusatzinformationen. Auf der »High End« in München präsentierten Bayern Digital Radio (BDR) und das IIS erstmals digitalen Hörfunk mit Multikanalton für Kopfhörer. Dabei wird die Klangübertragung zum Ohr simuliert. [Webkey 30502](#)

Simulationen für den Schiffsentwurf

St. Augustin. Schiffsbauer müssen unter hohem Zeit- und Preisdruck ständig neue Produkte entwickeln. Um die finanziellen Risiken zu begrenzen, entwickelt das Fraunhofer SCAI im Verbundprojekt SESIS ein System, das die frühe Entwurfsphase mit schnellen Simulations- und Entwurfstools unterstützt. Durch klar definierte, offene Schnittstellen können neue Simulationsmethoden ebenso wie bereits existierende genutzt werden. Vorhandene Anwendungsprogramme werden mittels Wrapper-Technologie eingebunden und können ebenfalls in vollem Umfang weiter verwendet werden. Außerdem wird die Zusammenarbeit interner und externer Entwickler durch eine einheitliche Datenablage und ein Versionsmanagement unterstützt. Um die Zulieferunternehmen einzubinden und die Entwurfsprozesse realistisch abzubilden, wird jetzt ein Demonstrator für ein exemplarisches Szenario aufgebaut und ein Betriebskonzept für die nachhaltige Nutzung entwickelt. [Webkey 30503](#)

Mathematik optimiert die Glasherstellung

Kaiserslautern. Technische Herausforderungen in der Glasherstellung und -verarbeitung lassen sich durch mathematische Modellierung und Simulation bestimmter Prozesse lösen. Themen der »Glass Days« in Kaiserslautern waren deshalb die optimale Steuerung und Glasabkühlung, die Simulation des Glaspessens und schnelle Algorithmen zum Wärmestrahlenstrahltransport. Die »Glass Days« bieten seit 10 Jahren ein Forum zur Lösung von Problemen rund um die Glasproduktion. [Webkey 30511](#)

Telematik statt Verkehrsinfarkt

Darmstadt. Ob Rockkonzert, Fußballweltmeisterschaft oder Olympische Spiele – internationale Großveranstaltungen sind eine Herausforderung für jede Verkehrslogistik: Verkehrsströme müssen rechtzeitig entflochten und situationsabhängig gesteuert werden. Für die Fußball-WM 2006 entwickeln zu diesem Zweck das Fraunhofer ISST und ein deutsch-chinesisches Forschungsteam einen digitalen Begleiter. Zahlreiche Dienste für Einzelnutzer, aber auch für das Verkehrsmanagement werden gebündelt auf einer gemeinsamen Plattform angeboten. Ein aktueller Dienst informiert die Besucher, wann sie spätestens aufbrechen sollten, berücksichtigt dabei die Verkehrssituation, den sich verändernden Standort sowie individuelle Vorlieben. Echtzeitdaten und Prognosen stellen sicher, dass alle Fans pünktlich zum Anpfiff die Stadien erreichen. Einmal eingeloggt, erhalten sie alle relevanten Verkehrsinformationen über Handy, PDA oder andere mobile Endgeräte.

30 Jahre Graphik

Darmstadt. Vor 30 Jahren wurde Professor Encarnaçao als Leiter des Fachgebiets Graphisch-Interaktive Systeme (GRIS) an die TU Darmstadt berufen. Aus dem damals neu gegründeten Forschungsbereich mit drei Mitarbeitern entstand das internationale Netzwerk »INI-GraphicsNET« mit über 900 Mitarbeitern. Auch das Zentrum für Graphische Datenverarbeitung, das Fraunhofer IGD sowie viele andere Institute weltweit sind aus GRIS hervorgegangen. Unter Encarnaçãos Leitung wurde das »INI-GraphicsNET« richtungsweisend für die Forschung an der Schnittstelle zwischen Mensch und Computer

Mobiles Europa

Berlin. Gemeinsam mit Nachrichtenagenturen aus fünf Ländern haben das Fraunhofer FOKUS sowie drei weitere technische Partner im EU-Projekt MIND mobile Informationsdienste und neue Geschäftsmodelle entwickelt. Präsentiert wurden jetzt im Fraunhofer FOKUS zehn Dienste aus den Bereichen Businessangebote, Multimedia-Entertainment, Nachrichtendienste, Community-Lösungen und Medienplattformen. [Webkey 30501](#)

Neues Klangerlebnis

Halle. Das Multimediazentrum in Halle wird im kommenden Jahr das am Fraunhofer IDMT entwickelte Soundsystem »IOSONO« einsetzen, und zwar sowohl für die Produktion im Studio als auch für die Präsentation in einem eigens ausgestatteten Kino. Hierfür wird eigens ein Tochterunternehmen gegründet: die IOSONO Produktion GmbH. Als nächste Generation des 5.1.-Sounds kann IOSONO mit einer Vielzahl von Lautsprechern »dreidimensionalen« Klang erzeugen und Geräusche an jedem Ort des Raums – und sogar außerhalb des Raumes – platzieren.

Hohe Auszeichnung

Erlangen. Der Medizininformatiker Bernd Blobel wurde zum »International Associate« des American College of Medical Informatics (ACMI) ernannt. Der Wissenschaftler vom Fraunhofer IIS erhielt die Auszeichnung für seine Forschungen über sichere und interoperable Gesundheitssysteme und Krankheitsakten in verschiedenen Ländern. Den Titel bekamen bisher nur 19 Wissenschaftler, darunter vier Deutsche.

► Weitere Informationen sowie einen tagesaktuellen Kalender finden Sie im Internet unter www.iuk.fraunhofer.de

DIGITALE MEDIEN

- 02.09.-07.09. Fraunhofer FIRST, FOKUS, IDMT, HHI, IIS und IZM präsentieren auf der »IFA« in Berlin Lösungen für **multimediales Leben**.
- 09.09.-13.09. Fraunhofer präsentiert auf der »IBC« in Amsterdam Kompressionsverfahren zur Verkürzung der Produktionszeiten beim **digitalen Kino**
- 28.09. Workshop »**Digital Multimedia Broadcasting** - ein vielversprechender Standard für Deutschland?« im Rahmen der Asia-Pazifik-Wochen in Berlin. (Fraunhofer FIRST)

E-BUSINESS

- 07.09.-08.09. Fraunhofer FIT und bureau42 GmbH veranstalten das »3. Symposium Zukunft **betrieblichen Wissens**« zum Thema Kompetenzmanagement
- 13.09. 3. Seminartag »Fit for Service – Dienstleistungen im Griff« über **Dienstleistungsunternehmen** von morgen. (Fraunhofer IAO)
- 23.09. Fraunhofer AIS feiert »Alumni- und Institutsfest« mit Executive Seminar »**Spatial Business Intelligence**«
- 27.10. Tagung »Professionalisierung **unternehmensinterner Dienstleistungen**« (Fraunhofer IAO)
- 15.11.-18.11. Fraunhofer IAO veranstaltet die »Stuttgarter E-Business Tage« zu Themen wie **Unternehmensportalen, Produktdatenmanagement** und **XML**

KOMMUNIKATIONSSYSTEME

- 07.08.-11.08. Das Fraunhofer AIS und die Universität Bonn veranstalten die »International Conference on **Machine Learning** (ICML)« in Bonn
- 14.09. Das deutsch-österreichische W3C-Büro veranstaltet zusammen mit den Berliner XML-Tagen den **W3C-Tag**
- 15.09.-16.09. Seminar »Future Meeting Room« zur **Planung von Kommunikationsräumen** (Fraunhofer IAO)
- 16.10.-20.10. Fraunhofer FIRST ist Mitveranstalter des »International Symposium on **Wikis**« im Rahmen der »OOPSLA-Konferenz« in San Diego, USA

KULTUR UND UNTERHALTUNG

- 13.09. Workshop zur **spielerischen Wissensvermittlung** (»Game-based Learning«) im Rahmen von DELFI und GMW (Fraunhofer IGD Rostock)
- 16.09.-02.10. **Fußballortungssystem** im Praxistest bei den »U-17-Weltmeisterschaften« in Peru (Fraunhofer IIS)

MEDIZIN UND LIFE SCIENCES

15.09. Seminar des Cast-Forums zum Thema »Smart Card« (Fraunhofer IGD)

PRODUKTION

09.11. Fachtagung des Fraunhofer IAO »Erfahrungswissen in der **Produktion** nutzen«

09.11. Seminar »Wettbewerbsfähig mit **Ganzheitlichen Produktionssystemen** - Von Praktikern für Praktiker« (Fraunhofer IAO)

09.11.-10.11. Fraunhofer ITWM auf den »20. Hofer **Vliesstofftagen**«

SECURITY

18.08. Seminar »**Forensik**« des Cast-Forums über Möglichkeiten der digitalen Spurensicherung (Fraunhofer IGD)

31.08. Seminar »**Sicherheitsmanagement** nach IT-Grundschutz« (Fraunhofer SIT)

31.08. Seminar »Entwicklung und Umsetzung von **Security Policies**« (Fraunhofer SIT)

03.09. Vortrag über **sichere Software** im Rahmen der Wissenstour der Zeitschrift P.M. in Berlin (Fraunhofer FIRST)

07.09. Seminar »Entwicklung und Umsetzung eines **Sicherheitskonzepts** nach IT-Grundschutzhandbuch« (Fraunhofer SIT)

08.09. Seminar »**Risiko- und Schwachstellenanalyse**« (Fraunhofer SIT)

09.09. INInnovation-Seminar der INI-GraphicsNet Stiftung »**Patente, Schutzrechte, Lizenzen**: Ihre Rolle in der Verwertung öffentlicher Forschung«

12.09.-16.09. Seminar »TeleTrusT **Information Security Professional** (TISP)« zur Erwerbung des Experten-Zertifikates TISP. (Fraunhofer SIT)

13.09.-16.09. Fraunhofer SIT ist Mitorganisator des »11th German-Japanese Symposium Security, Privacy and Safety in the Information Society« in Tokio, Japan

14.09.-15.09. Seminar »**Identitäts- und Berechtigungsmanagement**« (Fraunhofer SIT)

21.09. Seminar »**Security Awareness und Endanwendersicherheit**« (Fraunhofer SIT)

20-jähriges Jubiläum des Fraunhofer IIS



Erlangen. Das Fraunhofer IIS feierte am 30. Juni 2005 sein 20-jähriges Bestehen. Bekannt wurde das größte Fraunhofer-Institut mit der Erfindung des MP3-Musikformates. Das Jubiläum nimmt Institutsleiter Professor Heinz Gerhäuser zum Anlass, den Blick in die Zukunft zu richten: »Unser stetiges Wachstum und unsere Erfolge motivieren uns, neue Ideen mit Mut und Tatkraft in innovative Technologien umzusetzen. Wir wollen auch zukünftig Impulsgeber für die Wirtschaft sein und unsere Kompetenzen weiter ausbauen.« Im Zentrum stehen die Entwicklung von integrierten Schaltungen, die Informations- und Kommunikationstechnik sowie die Medizin- und Prüftechnik. Um die Forschungsaktivitäten örtlich zu konzentrieren, werden die Büro- und Laborkapazitäten des vor drei Jahren erstellten Institutsgebäudes in Erlangen verdoppelt.

Medienkunst ausgezeichnet

St. Augustin. Für ihre Medienkunstinstallation »Energie_Passagen« wurden die Fraunhofer-Wissenschaftler Monika Fleischmann und Wolfgang Strauss mit dem Industrie Forum Communication Design Award ausgezeichnet. »Energie_Passagen« ist ein begehrtes, auf die Straßen projizierbares Zeitungsarchiv. [Webkey 30504](#)

► Weitere Informationen sowie einen tagesaktuellen Kalender finden Sie im Internet unter www.iuk.fraunhofer.de

SECURITY

22.09. Seminar »**Sicherheitsmanagement** nach BS 7799 und ISO/IEC 17799« (Fraunhofer SIT)

28.09.-30.09. Intensivseminar »**Hacking** - Angriffsmethoden und Abwehrstrategien« (Fraunhofer SIT)

06.10. Seminar »Entwicklung sicherer **Web-Anwendungen**« (Fraunhofer SIT)

06.10. Informationstechnisches Kolloquium Karlsruhe »**Bildfolgeauswertung**« (Fraunhofer IITB)

19.10. Fraunhofer SIT veranstaltet zusammen mit dem BSI den »**IT-Grundschutztag**«

20.10. Seminar »**Virtual Private Network**« (Fraunhofer SIT)

20.10. Seminar des Cast-Forums zum Thema »**Enterprise Security**« (Fraunhofer IGD)

09.11.-11.11. Intensivseminar »**IT-Sicherheitsmanagement**« (Fraunhofer SIT)

09.11. Fraunhofer SIT auf dem »**Security Symposium**« des Telekomforums in Köln

01.12. SIT-Sicherheitsforum 2005 zum Thema »**Identity-Management**« in Darmstadt

SOFTWARE

15.11.-24.08. Fraunhofer FIRST und ISST veranstalten mit der BTU Cottbus das Software-Forum »**Service Oriented Architecture**« in Berlin

26.09.-29.09. Fraunhofer IESE veranstaltet ein Seminar zum Thema »**Quality Assurance in Reuse Contexts**« auf der »9th International Software Product Line Conference« in Rennes, Frankreich

15.11.-16.11. Fraunhofer IESE ist Mitveranstalter der »German DASMA MetriKon Conference« über **Software-Metriken** und Aufwandschätzverfahren in Kaiserslautern

VERKEHR UND MOBILITÄT

18.10.2005 Seminar »Effiziente Prozesse & innovative Lösungen in der **Kfz-Schadensregulierung**« (Fraunhofer IAO)

E-Government

28.10.2005 Das Fraunhofer eGovernment-Zentrum veranstaltet den Strategieworkshop »**eGovernment für die Wirtschaft**«

► Weitere Informationen sowie einen tagesaktuellen Kalender finden Sie im Internet unter www.iuk.fraunhofer.de

Frische Ideen braucht das Land

Rostock. Das Fraunhofer IGD hat erstmals den fachspezifischen Ideenwettbewerb »Computer Graphics 2005« veranstaltet. Forscher des Instituts sowie verbundener Einrichtungen waren aufgefordert, praxistaugliche Geschäftsideen einzureichen. Die Jury aus Vertretern der Wirtschaft prämierte die Video-Software von Dipl.-Inf. Mirko Ebert mit dem ersten Platz und 3.000 Euro Preisgeld. Mit der neuen Software können Nutzer sowohl Informationen in Videos hinzufügen als auch abrufen. So lässt sich Teamarbeit unter Mitarbeitern an mehreren Orten besser organisieren.

Europas Aktionsplan für mehr Sicherheit

Brüssel. Ein umfangreiches EU-Programm zur »Stärkung von Freiheit, Sicherheit und Recht« ist jetzt vom Rat »Justiz und Inneres« angenommen worden. Die Staats- und Regierungschefs hatten das so genannte »Haager Programm« bereits Ende 2004 abgesegnet. Die Vorhaben reichen von der Einführung neuer Reisepässe mit biometrischen Merkmalen über die Stärkung der Zusammenarbeit bei der Terrorismusbekämpfung bis hin zum Schutz von wichtigen Infrastrukturen. Nach Angaben des BITKOM sind viele der vorgesehenen Maßnahmen für die IT-Branche von Interesse, wie etwa die Einrichtung eines Informations- und Koordinierungsnetzes für Migrationsbehörden, Mindestnormen für die biometrische Identifikation in Personalausweisen, ein Visa-Informationssystem, Vorratsdatenspeicherung, Fingerabdruck-Datenbanken oder ein europäisches Strafverfolgungsnetz.

Forschung für multimediales Leben

Besuchen Sie uns auf der Internationalen Funkausstellung in Berlin (Halle 5.3)

Digital hören.

Alles fürs uneingeschränkte Hörvergnügen: Die Fraunhofer-Institute bieten kreative und effektive Lösungen für Urheberrechtsprobleme und arbeiten ständig an der Verbesserung der Klangqualität. Selbst auf mobilen Abspielgeräten ist jetzt Surroundqualität garantiert, und das Copyright steht dem Herunterladen von digitalen Produkten nicht mehr im Weg.

Interaktiv sehen.

Keine Leinwand, keine Maus und keine Bedienungsanleitung trennen den Menschen von der digitalen Welt: Mit Gesten gibt der Benutzer seinem Gerät Anweisungen, taucht in die dreidimensionalen Features ein und gestaltet sie intuitiv. Der digitale Raum gleicht sich der realen Welt immer mehr an und bietet so authentisches Multimediavergnügen.

Mobil agieren.

Zeit und Raum spielen bald keine Rolle mehr: Wo und wann man will, stehen dank der neuesten Fraunhofer-Entwicklungen Musik, Filme und elektronische Helfer in bester Qualität zur Verfügung. Auf dem Schreibtisch, am Flughafen und beim Sport trägt jeder Kino und HiFi-Anlage in der Westentasche, und der Golfball entpuppt sich als intelligenter Trainer.

Auf dem Fraunhofer-Stand erwarten Sie die Institute für Rechnerarchitektur und Softwaretechnik (FIRST), Nachrichtentechnik (Heinrich Hertz Institut, HHI), Digitale Medientechnologie (IDMT), Integrierte Schaltungen (IIS) und Zuverlässigkeit und Mikrointegration (IZM).

