

forschen



TECHNISCHE
UNIVERSITÄT
DARMSTADT

Sicherheit in einer digitalen Welt

IT-Risikomanagement

► Seite 12

Sichere Kommunikation
über unsichere Kanäle

► Seite 24

Physikalische
Fingerabdrücke gegen
Produktpiraterie

► Seite 42

Liebe Leserinnen und Leser,

die Wissenschaftsstadt

Darmstadt ist eine internationale

Hochburg der IT-Sicherheits-
forschung und -entwicklung.

Die Konzentration von exzellenter Lehre und produktiver, interdisziplinärer Forschung hat das Hessische Ministerium für Kunst und Wissenschaft 2008 in besonderer Weise ausgezeichnet: Im Rahmen seiner Landes-Offensive zur Entwicklung Wissenschaftlich-ökonomischer Exzellenz (LOEWE) ermöglicht es den Aufbau unseres Center for Advanced Security Research Darmstadt (CASED).

In den zwei Jahren seit der Gründung ist ein lebendiges Zentrum entstanden. Forscher der drei Trägerinstitute TU Darmstadt, Fraunhofer SIT und Hochschule Darmstadt haben sich eine neue Plattform geschaffen; eine Schnittstelle für vielfältige Kooperationen mit Partnern in Wissenschaft und Wirtschaft. Oder, wie es ein renommierter Gastredner unserer Distinguished Lecture Series kürzlich ausdrückte: „CASED ist zum größten Forschungszentrum für IT-Sicherheit in Europa angewachsen“. Diese schnellen Fortschritte verdanken wir der Vision, der kreativen Energie und der Leistung aller Beteiligten: der Wissenschaftlerinnen und Wissenschaftler, der Mitarbeiterinnen und Mitarbeiter von CASED und der unterstützenden Trägerinstitute.

In diesem Heft stellen die Autorinnen und Autoren Forschungsthemen vor, die gegenwärtig und in Zukunft unser Leben beeinflussen. Viele der heute eingesetzten und neu

entwickelten Technologien leisten in Geräten oder Software Erstaunliches und bleiben uns in ihrer Abstraktheit doch verborgen. Unsere Wissenschaftler arbeiten an der Sicherheit von IT und erhöhen die öffentliche Sicherheit durch IT. Neben den wissenschaftlichen Inhalten wollen wir auch die Köpfe hinter der Forschung vorstellen und der IT-Sicherheit an der TU Darmstadt und ihren Partnerinstitutionen ein – oder vielmehr – viele Gesichter geben. Die Autoren möchten Sie mit diesem Heft zu einem Blick in ihre Fachgebiete einladen. Zu allen Themen finden Sie Fachpublikationen und weitere Informationen auf den angegebenen Internetseiten.

Prof. Johannes Buchmann
Fachbereich Informatik
Fachgebiet Theoretische Informatik

CASED ist
laut Experten
zum größten
Forschungszentrum
für IT-Sicherheit
in Europa
angewachsen.

Dear Readers,

The scientific city of Darmstadt is an internationally renowned stronghold for IT security research and development, and the high concentration of excellent courses combined with productive, interdisciplinary research led to a special award by the Hessian Ministry for Science and the Arts in 2008: within the scope of its “Landes-Offensive zur Entwicklung Wissenschaftlich-ökonomischer Exzellenz (LOEWE – an initiative for developing scientific and economic excellence in Hessen)”, it has enabled the development of our Center for Advanced Security Research Darmstadt (CASED). CASED has now evolved into a vibrant center of research since it was founded two years ago. Researchers from the “Technische Universität Darmstadt”, the Fraunhofer Institute for Secure Information Technology (SIT) and the Darmstadt University of Applied Sciences, CASED’s three main supporting institutions, have developed a new platform for enabling versatile cooperation with partners from the worlds of science and business. Or, as a renowned guest speaker recently put it during a discourse held as part of our Distinguished Lecture Series: “CASED has grown into the largest research center for IT security in Europe”. This extremely fast development has been achieved thanks to the vision, the creative energy and the performance of all participants: the scientists and employees from CASED and the main supporting institutions.

In this book we will be introducing the authors who affect our lives today, and will continue to do so in the future. Many of the current and newly developed technologies perform amazing feats in devices and software, yet they remain hidden in their abstractness. Our scientists work on the security of IT and increase security in the public sphere through IT. In addition to the scientific content, we would also like to introduce the people behind the research and give a face (or many faces) to IT security at the TU Darmstadt and its partner institutions. The authors would therefore like to invite you to take a look inside their areas of expertise within this book. Specialist publications and further information on all of the topics presented can be found on the websites provided.



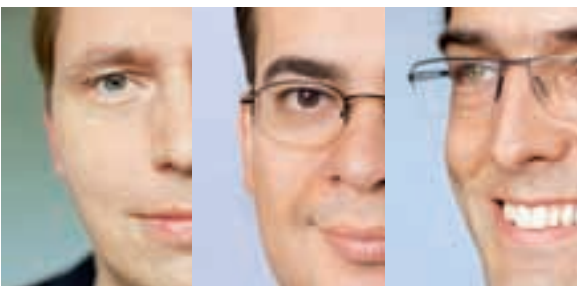
8 ► **Sicherheit in einer digitalen Welt**
Sicherheit in einer digitalen Welt:
Ein Überblick in die Zukunft und die Themen dieses Heftes.
Von **Johannes Buchmann**



12 ► **IT-Risikomanagement als wirtschaftlicher Erfolgsfaktor**
Ein Entscheidungsmodell hilft dabei, die Frage zu beantworten,
wie viel ein Unternehmen in IT-Sicherheit investieren und welche Systeme
geschützt werden sollten.
Von **Peter Buxmann, Tobias Ackermann**



16 ► **Sichere Produktdaten**
Entwicklung eines neuen Konzepts, um den Schutz von Produktdaten
zu verbessern und aktuelle Enterprise Rights Management-Lösungen entsprechend
den Anforderungen der Automobilindustrie zu bewerten.
Von **Reiner Anderl, Joselito Rodrigues Henriques**



24 ► **Sichere Kommunikation über unsichere Kanäle**
Sichere Kommunikation ist ein Eckpfeiler für
moderne Infrastrukturen wie das Internet.
Wie man sichere Kommunikation mittels
kryptographischer Methoden gewährleisten kann,
wird am CASED von mehreren Seiten beleuchtet.
Von **Marc Fischlin, Stefan Katzenbeisser, Mark Manulis**



30 ► **Quantenkryptographie – die Quantenphysik als Garant für sichere Kommunikation**
Die Quantenmechanik stellt die vermutlich erfolgreichste Theorie
in der Geschichte der Physik dar. Aber erst rund 100 Jahre
nach ihrer Entwicklung wird es möglich, ihre Gesetzmäßigkeiten
zur Anwendung zu bringen.
Von **Gernot Alber, Joseph M. Renes, Thomas Walther**



36

Adaptive Hardware für mehr IT-Sicherheit

Adaptive Hardware lässt sich dynamisch in ihrer Funktionalität verändern. Wie diese Eigenschaft gewinnbringend für mehr IT-Sicherheit verwendet werden kann, wird am CASED intensiv erforscht.

Von Sorin A. Huss, Andreas Koch, Sascha Mühlbach, Marc Stöttinger

42

Physikalische Fingerabdrücke gegen Produkt-Piraterie

Produktpiraterie ist ein schwerwiegendes und bisher ungelöstes Problem der heutigen Zeit. Einen neuen Lösungsansatz bieten PUFs (Physikalisch unklonbare Funktionen).

Von Frederik Armknecht, Ahmad-Reza Sadeghi



46

IT-Forensik – Technologie für Datendetektive

Dem missbräuchlichen Einsatz von IT zu begegnen, erfordert Methoden zur Erkennung, Rekonstruktion und Aufklärung. Das Fraunhofer-Institut für Sichere Informationstechnologie (SIT) entwickelt am CASED hierzu innovative Verfahren.

Von Martin Steinebach, Markus Schneider, Michael Waidner



50

Wolken und Datenspuren

IT-Sicherheit hat vielfältige rechtliche Bezüge. Anhand der beiden Forschungsgebiete „Cloud Computing“ und „IT-Forensik“ wird die rechtswissenschaftliche Forschung am CASED vorgestellt.

Von Alexander Roßnagel, Dennis Heinson, Mark Bedner

56

Sichere Netze – mit dem Nutzer im Zentrum

Der Schutz der Privatsphäre bei vernetzten Mobilfunk- und Internetanwendungen ist eine wichtige, aber bisher nur unzureichend gelöste Herausforderung.

Von Matthias Hollick, Thorsten Strufe, Alejandro Buchmann



Sicher fahren – Absicherung moderner Fahrzeugsoftware

60

Forscher an der TU Darmstadt entwickeln ein modellbasiertes Verfahren, um Verkehrsteilnehmer vor den Folgen von Angriffen auf die Fahrzeugsoftware zu schützen.

Von Sven Patzina, Lars Patzina, Eric Bodden, Mira Mezini, Andreas Sewe, Andy Schürr



Sicherheitsgarantien zuverlässig nachweisen

66

Die korrekte Funktionsweise von Software ist in vielen Anwendungsbereichen unabdingbar. Um derartige Zwischenfälle zu vermeiden, sollten kritische Aspekte von Softwaresystemen möglichst zuverlässig garantiert werden.

Von Heiko Mantel

IKT-Unterstützung erhöht Sicherheit in Stress-Situationen

72

Katastropheneinsätze bedeuten für die Einsatzkräfte vor Ort großen Stress. Innovative Informations- und Kommunikationstechnik für die Schnittstelle zwischen Mensch und Technik kann Ersthelfer in der Reaktionsphase unterstützen.

Von Dirk Bradler, Melanie Hartmann, Max Mühlhäuser, Ralph Bruder

Sicherheitskultur für eine digitale Welt

78

Neue Technologien verändern unseren Lebensalltag. Welche Fragen wirft das für uns und unsere Kultur auf und wie begegnen wir diesen vor, während und nach der Nutzung?

Von Christoph Hubig



Johannes
Buchmann

wissen, wo die entsprechenden Computer und Speichermedien stehen und wer sie kontrolliert. Das zukünftige Internet bringt Intelligenz in Straßen und Fahrzeuge. Es trägt dazu bei, Unfälle und Kosten, z. B. durch Verkehrsstaus zu ver-

meiden. In einer digitalen Welt wird Gesundheitsversorgung im häuslichen Umfeld auf hohem Niveau möglich. Gleichzeitig werden ihre Kosten gesenkt. Intelligente Produktionssysteme erlauben es besonders kleinen und mittleren

Unternehmen, gemeinsam Produkte und Dienstleistungen zu entwickeln und weltweit zu vermarkten. Solche Kooperationen finden im Internet statt und eröffnen ungeahnte neue Geschäftsmöglichkeiten.

Eine weitere, zentrale Aufgabe des heutigen und zukünftigen Internets ist der reibungslose Betrieb und Schutz unserer kritischen Infrastrukturen. Dazu gehören Energieversorgung, Kommunikation, Verkehr und Transport. In Katastrophensituationen ermöglicht das Internet schnelle und effektive Hilfe.

Sicherheit und Privatsphäre als Herausforderung

Die „digitale“ Welt wird sich nur entwickeln können und das Internet wird sein Potenzial nur dann voll entfalten können, wenn Sicherheit und Privatsphäre der Beteiligten gewährleistet sind. In Artikel 8 der Charta der Grundrechte der EU heißt es unter der Überschrift: Schutz personenbezogener Daten (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Sicherheit in dieser Form zu gewährleisten ist eine immense Herausforderung für Forschung und Entwicklung.

Kryptographie als Basis für IT-Sicherheitslösungen

Basis für jede IT-Sicherheitslösung sind kryptographische Verfahren, zum Beispiel Verschlüsselung. Verschlüsselung ermöglicht Vertraulichkeit. Die Erfahrung zeigt aber, dass Verschlüsselungsverfahren



Johannes Buchmann ist seit 1996 Professor am Fachbereich Informatik der TU Darmstadt. Er leitet das Fachgebiet Theoretische Informatik und ist Direktor des LOEWE-Zentrums CASED.

nach spätestens dreißig Jahren gebrochen werden können, zum Beispiel durch Quantencomputer, die heute diskutiert werden. Für langfristige Vertraulichkeit, die für viele Informationen im zukünftigen Internet erforderlich ist, zum Beispiel für medizinische Daten, reicht das nicht. Abhilfe kann hier nur mathematisch anspruchsvolle kryptographische Forschung oder vielleicht sogar die Quantenkryptographie schaffen. Ihre Sicherheit beruht auf der bedeutendsten Entdeckung der Physik des zwanzigsten Jahrhunderts, der Quantenmechanik. Viel Forschung wird aber noch nötig sein, bevor die Quantenkryptographie praktisch einsetzbar wird.

Die Entwicklung sicherer Kryptographie ist eine große Aufgabe und doch nur ein kleiner Schritt in Richtung eines sicheren Internets. Die komplexen Infrastrukturen des Internets mit den unzähligen Computern und Netzen wollen abgesichert werden und Sicherheitslösungen für die vielen Aufgaben des Internets müssen gefunden und implementiert werden.

So wird zum Beispiel in Zukunft der gesamte Lebenszyklus von Produkten von der Herstellung über Verkauf, Auslieferung, Wartung und Entsorgung im Internet gesteuert und überwacht. Dadurch wächst die Herausforderung, Produktfälschungen zu verhindern. Solche Herausforderungen führen zu komplexen Lösungen. Alle Sicherheit ist verloren, wenn bei der Implementierung der besten Sicherheitslösungen neue Sicherheitslücken eingebaut werden. So wird die Implementierung mit Sicherheitsgarantien zu einer weiteren wichtigen Disziplin.

Wie viel Sicherheit ist notwendig?

Sicherheit für das Internet ist eine *conditio sine qua non* – aber auch sehr teuer. Zu teuer? Darf es auch ein bisschen weniger Sicherheit sein? Die Beantwortung dieser Frage ist Aufgabe für viele nicht-technische Disziplinen. Welche Sicherheit ist unabdingbar? Was verlangen die Gesetze, und welche neuen Gesetze sind erforderlich? Welche Sicherheit wünschen sich die Bürger? Welche Sicherheit ist ökonomisch geboten und vertretbar?

Dieser Jahrhundertausforderung, Sicherheit für die zukünftige „digitale“ Welt und besonders das Internet der Gegenwart und Zukunft zu ermöglichen, widmet sich die interdisziplinäre Forschung und

Entwicklung in Darmstadt seit vielen Jahren in all ihren Dimensionen.

Mit dem Center for Advanced Security Research Darmstadt (CASED) ist Darmstadt inzwischen zum größten europäischen Forschungs- und Ausbildungszentrum für Internet- und IT-Sicherheit geworden. Ermöglicht wurde dies durch die hessische Landes-Offensive zur Entwicklung wissenschaftlich-ökonomischer Exzellenz (LOEWE). Die drei führenden Darmstädter Institutionen für IT-Sicherheit, die TU Darmstadt, das Fraunhofer Institut für Sichere Informationstechnologie SIT und die Hochschule Darmstadt, haben sich im LOEWE-Exzellenzwettbewerb behauptet und konnten im Juli 2008 CASED als eines von fünf LOEWE-Zentren gründen.

IT-Sicherheitsstandort Darmstadt

In weniger als zwei Jahren wurden für CASED fünf neue international renommierte Professoren berufen, mehr als sechzig Wissenschaftlerinnen und Wissenschaftler für die Mitarbeit gewonnen und ein neuer Master-Studiengang IT-Sicherheit an der

TU Darmstadt etabliert. Große Unternehmen wie die Darmstädter Software AG und die SAP AG sind Partner von CASED. Aber auch viele mittelständische Firmen, die sich auf IT-Sicherheit spezialisiert haben wie Kobil Systems und die USD AG. Die CASED-Exzellenz hat sich in weiteren Wettbewerben bewiesen: CASED vertritt im BMBF-Spitzencluster „Softwareinnovationen für das digitale Unternehmen“ schwerpunktmäßig die IT-Sicherheitsforschung und ist Sitz seiner Koordinierungsstelle. Auf internationaler Ebene beteiligt sich CASED an der europäischen Exzellenzinitiative European Institute of Innovation and Technology (EIT).

Die Artikel dieses Heftes geben einen Eindruck von der Spannweite der Darmstädter IT-Sicherheitsforschung und -Entwicklung.

Fachgebiet Theoretische Informatik – Kryptographie und Computeralgebra

Prof. Dr. Johannes A. Buchmann

Tel. 06151/16-3416

E-Mail: buchmann@cdc.informatik.tu-darmstadt.de

www.cdc.informatik.tu-darmstadt.de

ANZEIGE



KLEINE DINGE, GROSSE WIRKUNG

Wo sich kluge Köpfe treffen, werden oft bahnbrechende Ideen geboren. Und manchmal sind es nur relativ kleine Dinge, die den Ausschlag für eine große Idee geben: Inspirierende Architektur, die perfekte Präsentationstechnik, eine Atmosphäre einfach zum Wohlfühlen.

Das darmstadtium wissenschaft | kongresse –
Treffpunkt für die Macher der Märkte von morgen.




darmstadtium
wissenschaft | kongresse
www.darmstadtium.de

IT-Risikomanagement

als wirtschaftlicher Erfolgsfaktor

Die meisten Unternehmen sind schon einmal Opfer von IT-Sicherheitsangriffen geworden. Dahinter stecken häufig wirtschaftliche oder auch politische Motive; manchmal aber auch nur „Spaß“ oder Langeweile von Jugendlichen. Die Schadenshöhe kann für Unternehmen existenzgefährdend sein. Umso erstaunlicher ist, dass in den meisten Unternehmen Wirtschaftlichkeitsüberlegungen zum IT-Risikomanagement kaum eine Rolle spielen. Aber wie viel sollte ein Unternehmen eigentlich in IT-Sicherheit investieren und welche Systeme sollten ausgewählt werden? Vor diesem Hintergrund entwickeln wir ein Entscheidungsmodell für das Management von IT-Risiken.

► IT Risk Management as economic factor of success

Most companies already fell victim to IT security attacks. Often, these attacks are motivated economically or politically, but sometimes they are done by young people just for fun or out of boredom. The potential losses can jeopardize whole businesses and it is remarkable that most companies do not consider economic aspects in their IT risk management. But how much should a company invest in IT security and what systems should be secured? Against this background, we develop a decision model for the management of IT risks.

Peter Buxmann, Tobias Ackermann • Die zunehmende Vernetzung und die rasante Fortentwicklung der Informations- und Kommunikationstechnologie haben die Gesellschaft und die Unternehmenswelt nachhaltig verändert. So ist die IT-Unterstützung von inner- und zwischenbetrieblichen Geschäftsprozessen heute genauso eine Selbstverständlichkeit wie das Googeln nach Informationen oder die mobile Nutzung von Apps. Es entstehen ständig neue Plattformen, Anwendungen und Dienste – und damit auch immer neue Sicherheitsrisiken.

Neben „Worst case-Szenarien“, wie wir sie beispielsweise aus vielen Spielfilmen kennen, in denen es Terroristen gelingt, die Gewalt über Computersysteme zur Steuerung von Verkehrssystemen, Atomkraftwerken oder Energieversorgungssystemen zu übernehmen, ist die Liste von Sicherheitslücken und -vorfällen lang und betrifft unterschiedlichste Bereiche.

So kommt es immer wieder vor, dass Unternehmen nicht mehr auf ihre Anwendungen und Daten zugreifen können. Selbst großen und in der Regel

hochprofessionell arbeitenden Anbietern gelingt es nicht immer, Systemabstürze zu vermeiden. Dies zeigen beispielsweise die Server-Ausfälle bei Amazon, Google und Salesforce.com. Die Kosten für Ausfallzeiten in Unternehmen sind branchenabhängig unterschiedlich hoch. So setzen Studien beispielsweise die Ausfallkosten in der Logistik auf 90.000 Euro an, während sie für Online-Broker-Systeme auf 6,5 Millionen Dollar geschätzt werden – pro Stunde Downtime. Zu den unmittelbaren Ausfallkosten kommen außerdem die schwer zu quantifizierenden Schäden durch Imageverlust bei verärgerten Kunden und Lieferanten hinzu.

Andere Sicherheitsvorfälle betreffen den Verlust oder die Verletzung der Vertraulichkeit von Kundendaten. Bei T-Mobile USA wurden beispielsweise Daten von tausenden Sidekick-Nutzern durch einen Serverfehler gelöscht und konnten teilweise nicht wieder hergestellt werden. Heise titelte: „Ein Schatten legt sich auf die Cloud“. Bei der Internet-Jobbörse Monster wurden Datensätze von mehr als 4,5 Millionen Betroffenen gestohlen, die unter anderem sensible Informationen wie Passwörter, E-Mail-Adressen, Namen und Telefonnummern enthielten. Viele Social-Network-Plattformen lassen sich relativ leicht hacken, um Zugriff auf persönliche Daten, wie Freundeslisten, Gästebücher etc. zu erhalten. Die Attacken sind zum Teil wirtschaftlich, teilweise aber auch politisch motiviert, wie der Hackerangriff auf Google in China zeigt.

Eine Studie des Ponemon Instituts schätzt, dass ein durchschnittlicher IT-Sicherheitsvorfall zu einem Schaden von 6,75 Mio. US-Dollar führt. In einer Umfrage gaben über zwei Drittel der befragten Unternehmen an, dass sie bereits Opfer von Internetangriffen wurden, z. B. durch Malware wie Viren, Würmer und Trojaner oder „Denial of Service“-Angriffe. Ein Drittel dieser Attacken war erfolgreich. Zu den Folgen zählten Ausfallzeiten, Diebstahl von

Fachgebiet Information Systems/Wirtschaftsinformatik
Prof. Dr. Peter Buxmann
Tel. 06151/16-4826
E-Mail: buxmann@is.tu-darmstadt.de

Dipl.-Wirtsch.-Inform. Tobias Ackermann
Tel. 06151/16-70473
E-Mail: tobias.ackermann@cased.de
www.is.tu-darmstadt.de

Peter Buxmann



Mitarbeiter- oder Kundendaten sowie der Verlust von Kreditkarteninformationen.

Umso erstaunlicher ist es vor diesem Hintergrund, dass Entscheider der wirtschaftlichen Analyse von Investitionen zur Vermeidung bzw. Reduzierung von IT-Risiken offenbar eine relativ geringe Bedeutung beimessen. So gaben in einer Studie unter 1.000 IT-Entscheidungsträgern etwa die Hälfte an, keine Kenntnisse über potenzielle Schadenshöhen aufgrund von Sicherheitslücken zu haben.

Interessanterweise steigt die Sensibilität der Unternehmen für das Thema Sicherheit, wenn Daten oder auch Prozesse nach außen gegeben werden sollen, etwa an Outsourcing-, Software-as-a-Service- (SaaS) oder Cloud-Computing-Anbieter. Im Rahmen mehrerer empirischer Untersuchungen der Software Economics Group Darmstadt-München haben wir Anwender nach den Chancen und Risiken des Einsatzes von SaaS befragt. Dabei sind gemäß einer Befragung von 349 IT-Entscheidungsträgern die (subjektiv wahrgenommenen) IT-Risiken zurzeit der wichtigste Grund, nicht auf solche SaaS-Lösungen umzusteigen. Interessant ist, dass SaaS-Kunden und Nicht-Kunden diese Risiken unterschiedlich bewerten. Nicht-Kunden betrachten SaaS noch mit Argusaugen und trauen dem Fremdbezug von IT-Diensten noch nicht so richtig über den Weg. Diejenigen Firmen, die sich jedoch für eine SaaS-Nutzung entschieden haben, bewerten die Risiken durchwegs geringer.

Flankierend haben wir Fallstudien zur Bereitschaft der Verlagerung von Diensten nach außen geführt, die zeigen, dass insbesondere kleine und mittlere Unternehmen zögern, Services und Daten nach



Peter Buxmann ist Professor für Wirtschaftsinformatik an der Technischen Universität Darmstadt und befasst sich u. a. mit den Spielregeln der Softwareindustrie, Software-as-a-Service und IT-Sicherheit. Er ist zudem Principal Investigator des LOEWE-Zentrums CASED.



Tobias Ackermann ist wissenschaftlicher Mitarbeiter am Fachgebiet Information Systems/Wirtschaftsinformatik an der TU Darmstadt und Stipendiat der CASED-Graduiertenschule.

IT-Risikomanagement

Der IT-Risikomanagementprozess wird meistens als Vorgehensweise bestehend aus vier Phasen beschrieben: Die Identifikation hat die Ermittlung unternehmensrelevanter Bedrohungen zum Ziel. In der Phase der Quantifizierung werden für die Bedrohungen die beiden Größen Eintrittswahrscheinlichkeit und Schadenshöhe geschätzt. Die Steuerung der Risiken erfolgt durch gezielte Implementierung von Gegenmaßnahmen, während die Kontrolle dazu dient, die Entscheidungen in den vorangegangenen Phasen zu evaluieren. IT-Risikomanagement ist ein kontinuierlicher Prozess, da sich die Werkzeuge der Angreifer, aber auch die verfügbaren Sicherheitstechnologien ständig weiterentwickeln.

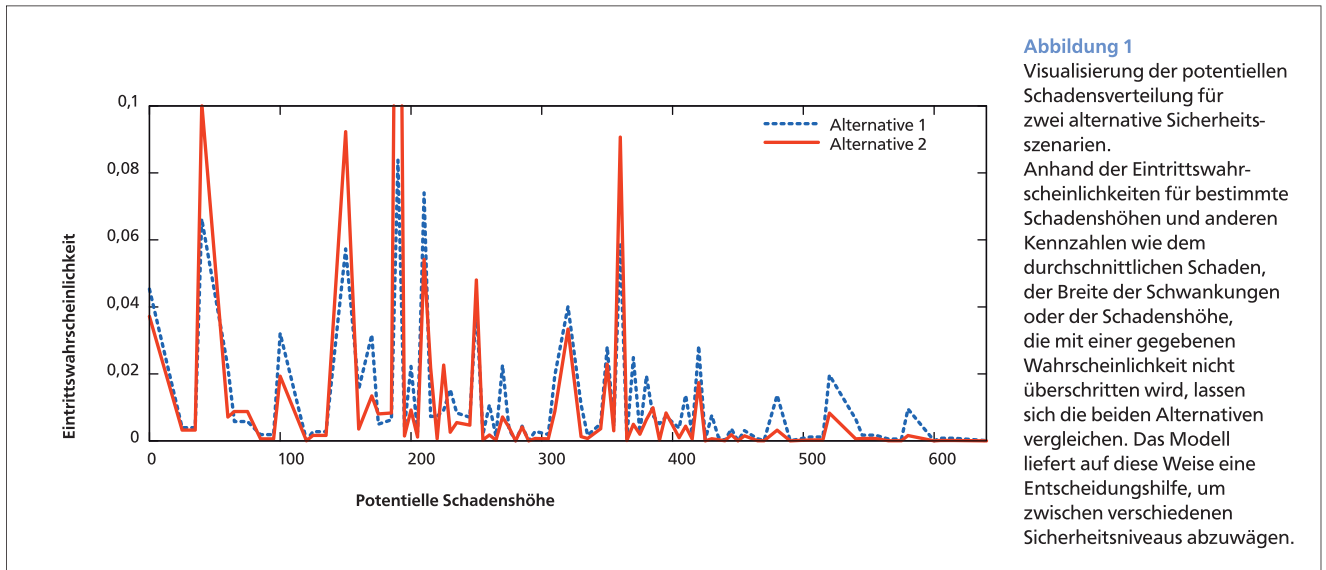
außen zu verlagern. Diese Skepsis verstärkt sich, wenn es darum geht, Daten und Prozesse an Off-shore-Standorte zu verlagern.

Ein Entscheidungsmodell zum Management von IT-Risiken

Vor diesem Hintergrund haben wir im Rahmen unseres CASED-Teilprojekts ein Modell zum Management von IT-Risiken entwickelt. Das Ziel besteht darin, Anwendern eine Entscheidungshilfe bei der Auswahl alternativer Maßnahmen zum IT-Risikomanagement zur Verfügung zu stellen. Ausgangspunkt ist eine Modellierung der Geschäftsprozesse der beteiligten Unternehmen. Im Anschluss werden auf Basis eines Risikokatalogs für die Funktionen der Prozesse sowie die Kommunikation zwischen diesen Sicherheitslücken identifiziert. Darauf aufbauend werden für die identifizierten Risiken das Schadensausmaß für verschiedene Szenarien und die jeweiligen Eintrittswahrscheinlichkeiten geschätzt.

Entscheidend für die Anwendung des Modells in der Praxis ist die Bestimmung der Parameter. Um möglichst realistische Werte zu erhalten, arbeiten wir am CASED eng mit Juristen und Informatikern zusammen. Rechtswissenschaftler können beispielsweise helfen, Prozesskosten für alternative Szenarien abzuschätzen.

Informatiker wiederum bringen fundiertes Wissen über die Wahrscheinlichkeit ein, mit der bestimmte



Systeme ausfallen oder gebrochen werden. Das Modell erlaubt auch die Abbildung von Prozessen im „Internet of Services“, bei denen Dienste unterschiedlicher Anbieter zu einer auf die Bedürfnisse der Kunden zugeschnittenen Lösung kombiniert werden.

Auf Grundlage des Entscheidungsmodells ist es möglich, alternative Investitionen in IT-Sicherheit zu bewerten und auszuwählen. Beispielsweise lässt sich abwägen, ob eine zusätzliche Ende-zu-Ende-Verschlüsselung eingesetzt werden sollte oder ob Standard-Verfahren wie SSL ausreichend sind, um die Vertraulichkeit von Daten zu schützen. Mit Hilfe von Modellanalysen lässt sich zeigen, dass aus ökonomischer Sicht ein optimales Sicherheitsniveau existiert, das häufig nicht dem technischen entspricht.

Aber nicht nur auf Nutzerseite lassen sich mit Hilfe des Modells Entscheidungen unterstützen. So gilt grundsätzlich, dass Unternehmensstrategien, auf die Kundenbedürfnisse abzustimmen sind.

Konkret betrifft das die Preis-, Produkt-, Vertriebs- und Kommunikationspolitik. Die Idee besteht also darin, Sicherheitsmechanismen in die Herstellerstrategien zu integrieren. So könnten die Anbieter auf Basis der Risikopräferenzen und Zahlungsbereitschaften der Kunden beispielsweise eine Preis- und Produktdifferenzierung etablieren. Dabei handelt es sich um eine bewährte strategische Maßnahme, um die unterschiedlichen Zahlungsbereitschaften verschiedener Kundengruppen abzuschöpfen. Darüber hinaus könnten die Anbieter das Thema IT-Sicherheit bzw. die Maßnahmen, um diese zu gewährleisten, in ihre Kommunikationsstrategie integrieren. Auf diese Weise bietet sich ihnen die Chance das notwendige Vertrauen aufzubauen, um Neukunden zu gewinnen bzw. bestehende Kunden an sich zu binden. Dies könnte insbesondere auch für deutsche IT-Sicherheitsfirmen von Interesse sein, die in der international geprägten Softwareindustrie bislang nur eine Nebenrolle spielen.

Praxisprojekte

- Im Rahmen des BMBF-Projekts Premium Services werden u. a. in Kooperation mit SAP Research und dem Fraunhofer-Institut SIT die Nutzerpräferenzen und Zahlungsbereitschaften für einen dort entwickelten Sicherheitsdienst untersucht. Die Ergebnisse sollen als Eckdaten für die ökonomische Entwicklung von IT-Sicherheitsstrategien aus Anbietersicht genutzt werden.
- Für die Darmstädter Momax GmbH wurde eine wirtschaftliche Risiko- und Sicherheitsevaluation ihres Micropayment-Systems miniPay durchgeführt. Der Zahlungsdienst ermöglicht es seinen Kunden, beispielsweise Verlagen, digitale Inhalte an Endkunden auf

einfache Art per Lastschrift zu verkaufen. Im Rahmen des Projektes wurden die Systemkomponenten, deren Zusammenspiel untereinander und die verwendeten Protokolle für den Zahlungsablauf systematisch untersucht und bewertet.

- In Kooperation mit einem Praxispartner aus dem öffentlichen Bereich wurde ein Entwurf eines IT-Sicherheitskonzepts für einen Teilbereich der IT-Landschaft erstellt. Dieses Dokument enthält eine individuelle Analyse möglicher Angriffs- und Schadensszenarien und empfiehlt Maßnahmen, um ein definiertes Schutzniveau zu erreichen.

Sichere Produktdaten

Um ihr geistiges Eigentum zu schützen, müssen Unternehmen vor allem die Sicherheit von digitalen Produktdaten im Produktentwicklungsprozess gewährleisten können. Dafür geeignete Verfahren können wirtschaftlichen und technischen Schaden durch Datenspionage verhindern. Wissenschaftler der TU Darmstadt entwickeln am CASED ein neues Konzept, um den Schutz von Produktdaten weiter zu verbessern und untersuchen aktuelle Enterprise Rights Management (ERM)-Lösungen in Hinblick auf die Anforderungen der Automobilindustrie.

► Secure Product Data

In order to keep the intellectual property of a company protected, product data has to be protected during the product development process.

Appropriate techniques avoid economical and technical damage caused by data espionage. At CASED, a new concept to improve product data protection is being developed, and current Enterprise Rights Management solutions are evaluated in respect to the requirements of the automotive industry.

Reiner Anderl, Joselito Rodrigues Henriques • Im Ingenieurwesen ist der Einsatz des rechnergestützten Konstruierens (Computer Aided Design, CAD) in der Produktentwicklung nicht mehr wegzudenken. Es steckt viel schützenswertes Wissen – geistiges Eigentum (Intellectual Property, IP) – in den CAD-Daten, das sich einfach speichern, reproduzieren und in die Prozesskette integrieren lässt – und auf das leicht zugegriffen werden kann. Einerseits beschleunigt die Integration von Firmen-Know-how in CAD-Daten die Produktentwicklung und ermöglicht die Zusammenarbeit von verschiedenen Unternehmensbereichen, etwa von Entwicklung und Produktion. Andererseits steigt das Risiko für Unternehmen, wenn sie die CAD-Daten neben den internen Abteilungen auch externen Partnern zur Verfügung stellen müssen. Heute regeln die meisten Unternehmen die Nutzung und Weitergabe ihrer Unternehmensdaten durch Partner nur durch Geheimhaltungsvereinbarungen, Gesetze und technische Maßnahmen. Diese aber können die Sicherheit der Daten nicht garantieren. Sobald die Daten das Unternehmen verlassen, hat der Urheber keine Möglichkeit mehr, sie zu kontrollieren. Ohne den effizienten Schutz von Produktdaten steigt der durch Industriespionage und Produktpiraterie verursachte Schaden weiter an.



Reiner Anderl

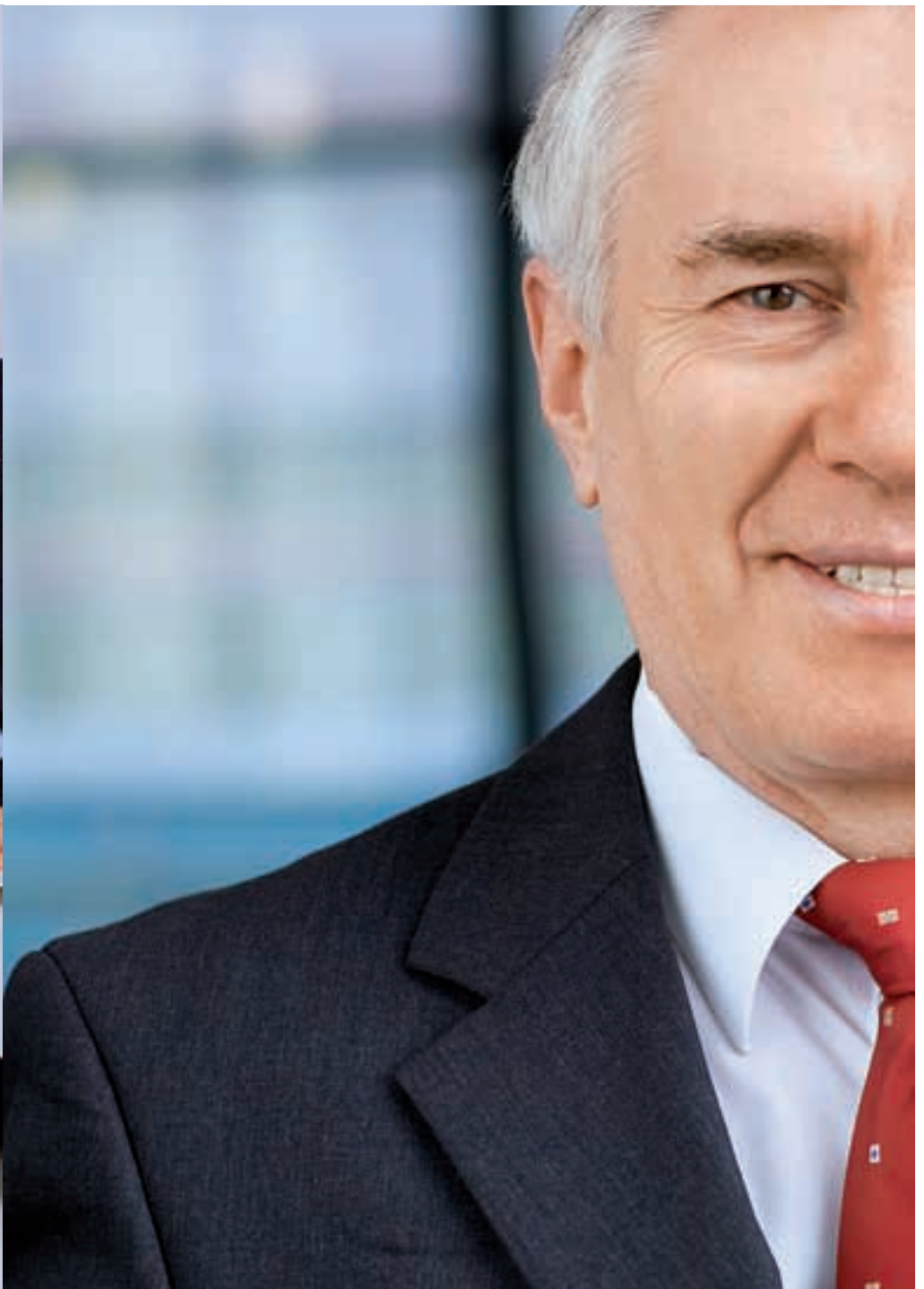
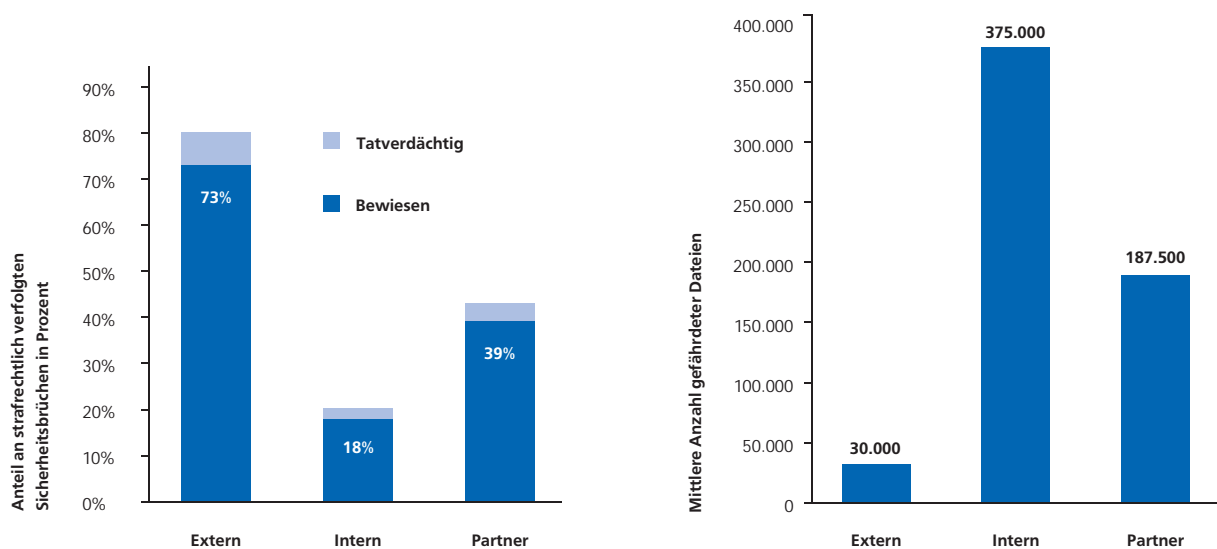


Abbildung 1

Verursacher von Sicherheitsbrüchen und Anzahl der gefährdeten Dateien



Nach einer von der Business Risk & Crisis Management GmbH durchgeführten Studie aus dem Jahr 2007 kostet Industriespionage deutsche Unternehmen jedes Jahr zirka 20 Milliarden Euro. Über 500 Fälle von Datenspionage über einem Zeitraum von vier Jahren wurden einer forensischen Untersuchung des Verizon Business Risk-Teams zufolge gemeldet. Abbildung 1 zeigt das Ergebnis einer Analyse, in der die Verursacher von Sicherheitsbrüchen und die Anzahl der gefährdeten Dateien aufgeführt werden.

Um die Sicherheit der gemeinsam genutzten Daten zu garantieren, kann man beispielsweise sicherstellen, dass nur befugte Personen auf verteilte Daten zugreifen können. Dies kann durch die ERM-Technologie (Enterprise Rights Manage-

ment) gewährleistet werden, wobei die Daten bereits bei ihrer Erstellung geschützt werden. Für den Schutz von CAD-Daten ist die Integration von ERM-Lösungen jedoch neu. In CATIA zum Beispiel, einem der wichtigsten in der Automobilindustrie eingesetzten CAD-Systeme, wurde die ERM-Technologie 2007 eingeführt. Produktdaten werden mithilfe aktueller ERM-Lösungen zwar sicherer, trotzdem kann darin enthaltenes geistiges Eigentum aber noch nicht ausreichend geschützt werden. Aus diesem Grund arbeitet das Fachgebiet „Datenverarbeitung in der Konstruktion DIK“ am CASED daran, die aktuelle ERM-Technologie zu verbessern und somit die Verarbeitung von digitalen Produktdaten sicherer zu gestalten.

Produktdaten

Viel Firmen-Know-how lässt sich heute digital in CAD-Dateien speichern: Neben grundlegenden Informationen über die Geometrie werden verschiedene Arten von Produktinformationen in CAD-Dateien gespeichert. Dazu zählen hochsensible Informationen, wie Modellierungs- und Konstruktionsstrategien, Produktionsinformationen

Fachgebiet Datenverarbeitung in der Konstruktion

Prof. Dr.-Ing. Reiner Anderl
Tel. 06151/16-6001
E-Mail: anderl@dik.tu-darmstadt.de

M.Sc. Joselito Rodrigues Henriques
Tel. 06151/16-50778
E-Mail: joselito.henriques@cased.de
www.dik.tu-darmstadt.de

und Konstruktionsmerkmale sowie Produkteigenschaften und Materialdaten. Eine weitere Form von geistigem Eigentum in CAD-Dateien sind Wissensmodelle, die in der wissensbasierten Konstruktion (Knowledge Based Engineering, KBE) eingesetzt werden. Mithilfe von KBE können Konstrukteure intelligentere digitale Produktrepräsentationen erzeugen, indem sie in die Bauteildateien komplexe Gleichungen, Parameter, topologische Informationen und andere Informationen einbinden. Mit der Integration von KBE in den Produktentwicklungsprozess werden Zeit und Kosten der Produktentwicklung in erheblichem Umfang reduziert. Die sich ergebende Produktstruktur wird in Abbildung 2 dargestellt.

Aktuelle technische Ansätze zum Schutz von Produktdaten

Die aktuellen Methoden, das geistige Eigentum der Firmen zu schützen, erfüllen nicht alle Anforderungen

der Industrie. Es gibt zum Beispiel nach wie vor keine Möglichkeit, die CAD-Daten auf feingranularer Ebene zu schützen. Dies ist aber wichtig für die sichere Zusammenarbeit mit internen und externen Partnern im Produktentwicklungsprozess. Im Folgenden werden einige der aktuell eingesetzten Verfahren zum Schutz von Produktdaten vorgestellt und die möglichen Schwachstellen erläutert.

Terminalserver

Terminalserver ermöglichen es, die vollständige Kontrolle über Daten zu gewährleisten, da sie nur per Fernzugriff verarbeitet werden können. Sie können aber nur eingesetzt werden, wenn die relevanten Daten dem Unternehmen des Benutzers gehören und nur intern verwendet werden. Diese technische Methode ist hilfreich, um geistiges Eigentum innerhalb des Unternehmens zu schützen. Sie deckt allerdings nicht den in der Firmenkooperation essenziellen Datenaustausch ab (Abbildung 3a).

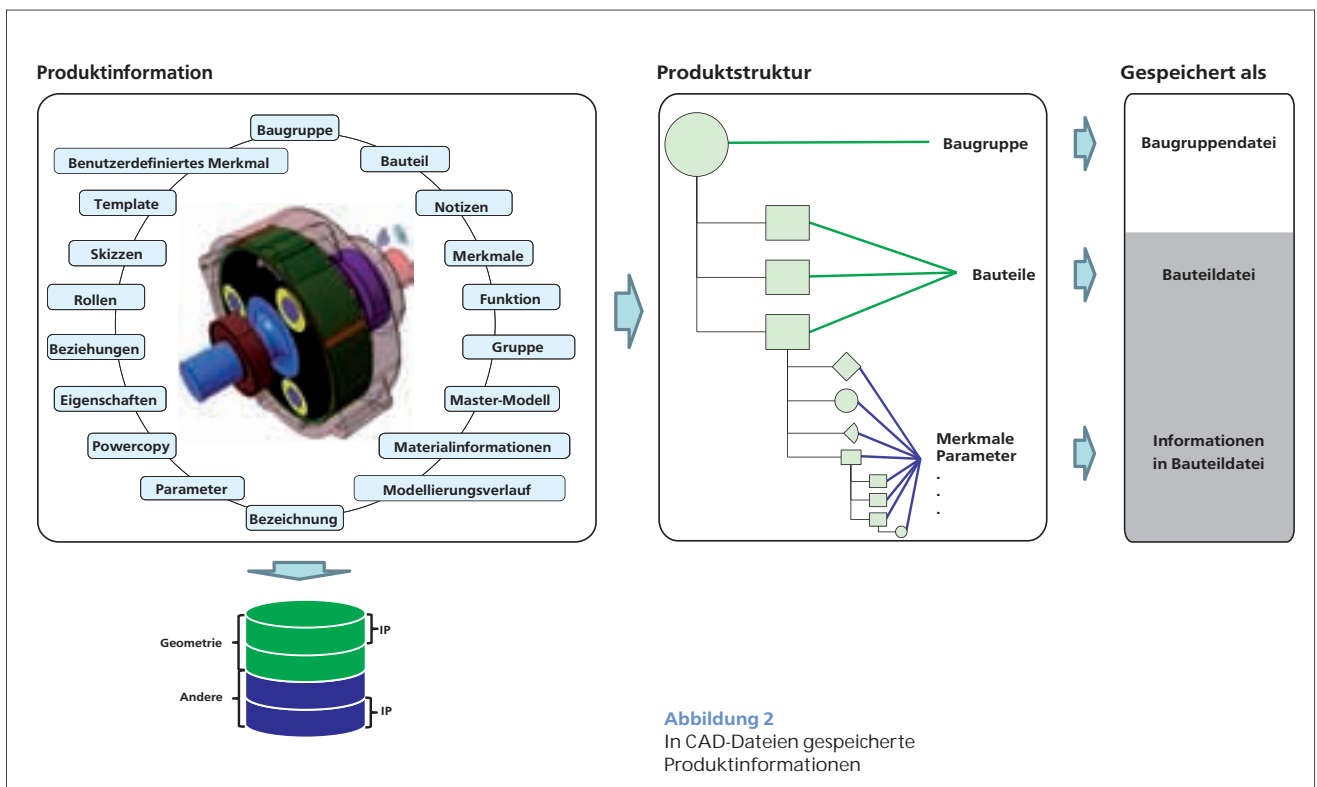
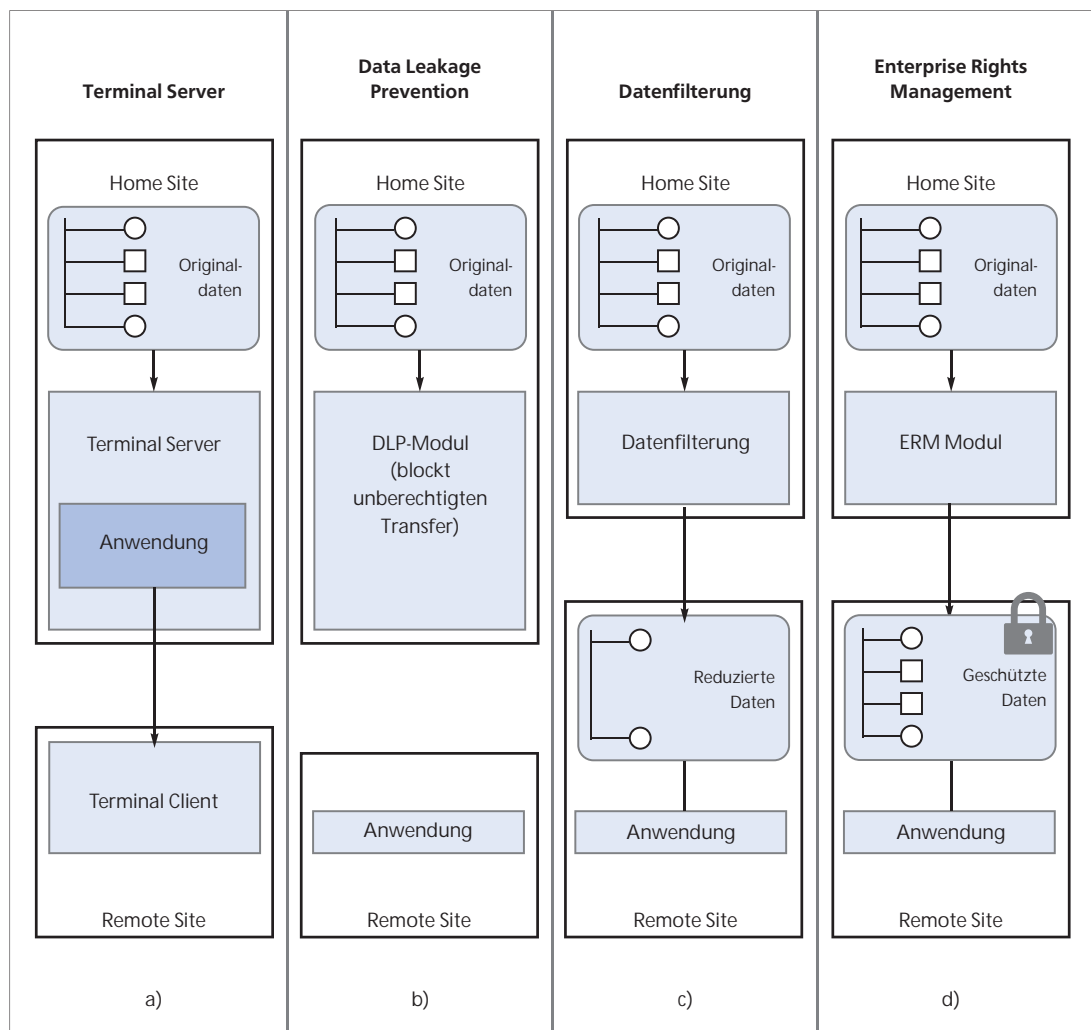


Abbildung 2
In CAD-Dateien gespeicherte Produktinformationen

Abbildung 3
Technische Ansätze
zum Schutz von
geistigem Eigentum



Data Leakage Prevention (DLP)

Bei dieser Methode wird durch spezielle Software auf dem Anwendersystem kontrolliert, welche Daten über welche Schnittstellen (zum Beispiel E-Mail, über Netzwerk oder externe Speichergeräte) übertragen werden dürfen. Diese Lösung ist sehr komplex, da der Schutz von Daten nur dann vollständig gewährleistet ist, wenn die komplette Softwareumgebung der Benutzer kontrolliert wird. Sobald auch nur eine unüberwachte Schnittstelle vorliegt, und Daten darüber kopiert werden oder das Unternehmen im Rahmen des Datenaustauschs verlassen, kön-

nen sie ungehindert weiter verteilt werden (Abbildung 3b).

Datenfilterung

Diese Methode reduziert den Wissensinhalt in den CAD-Daten, indem sensible Informationen gelöscht werden. Datenfilterung ist eine effiziente Methode, um geistiges Eigentum beim Datenaustausch zu schützen. Allerdings ist sie wiederum nicht dafür geeignet, um geistiges Eigentum innerhalb des Unternehmens zu schützen. Darüber hinaus erlaubt die Methode nicht, jene Informationen zu kontrollieren, die nicht gelöscht wurden

und so immer noch das Unternehmen verlassen (Abbildung 3c).

ERM – Enterprise Rights Management

Bei dieser Methode werden die Daten bereits bei der Erstellung geschützt und überwacht. Der Schutz bleibt während des gesamten Lebenszyklus erhalten. Heute ist dies die einzige Methode, die geistiges Eigentum prinzipiell innerhalb und außerhalb des Unternehmens effizient schützen kann. Allerdings ist heute ein Schutz per ERM nur auf Dateiebene möglich. In den Dateien befindliche Informationen können bisher nicht selektiv

auf feingranularer Ebene geschützt werden; sobald Zugriffsrechte für eine Datei bestehen, wird dadurch deren Wissensinhalt vollständig zugänglich.

Es ist offensichtlich, dass keine der bisherigen Methoden alleine sicheren Schutz von digitalen Produktdaten gewährleisten kann. Eine Kombination der Ansätze der genannten Methoden kann die gewünschte Sicherheit ermöglichen. Als effiziente Lösung wird die Weiterentwicklung der ERM-Technologie angesehen, die um feingranularen Schutz für verschiedene Datenebenen und Benutzer erweitert werden kann (Abbildung 3d).

ANZEIGE



The European Space Agency provides for and promotes cooperation amongst European States in space science, research and technology and their space applications. ESA works exclusively for peaceful purposes.

For over three decades the 18 countries of ESA have been pooling their resources to create a dynamic programme of space exploration and technology. Europe's most brilliant scientists and skilled engineers have brought space into our lives through diverse and dynamic means, in the fields of : - Exploration of the solar system and deep space - Launchers - Human space flight and space laboratories - Earth observation and meteorology - Satellite communications - Satellite navigation systems.

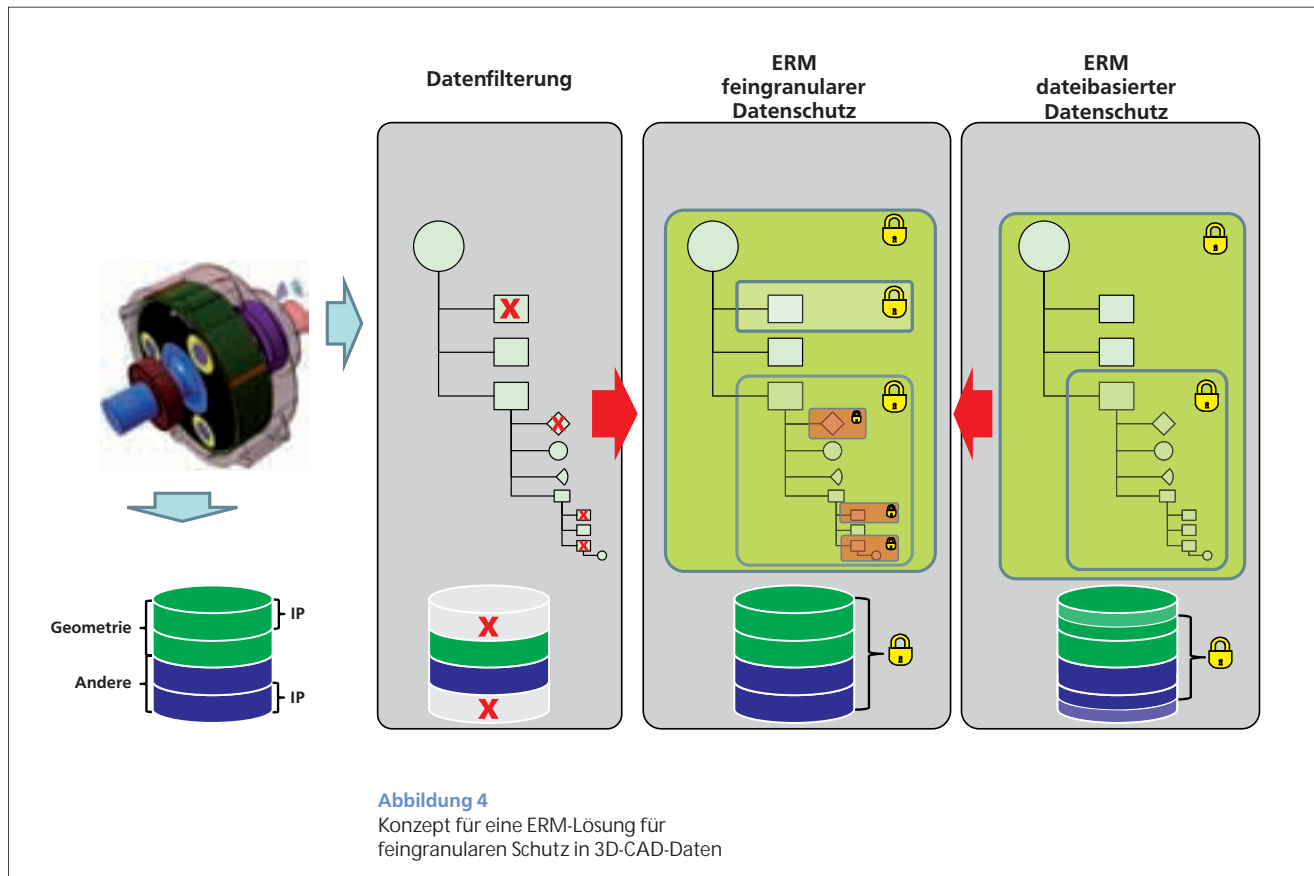
ESA is organised in a number of key "centres" - ESA is headquartered in Paris. ESA's technology centre (ESTEC) is located in Holland. The data processing centre (ESRIN) is located in Italy. The astronaut centre (EAC) and the satellite operations centre (ESOC) are located in Germany.

The European Space Agency is continuously looking to recruit aerospace, electrical and mechanical engineers, IT specialists, physicists, mathematicians, astronomers, and astrophysicists. Types of employments encompass a variety of areas: research and development, project support, project management, spacecraft operations and data retrieval and exploitation.

ESA/ESOC

Robert-Bosch-Str. 5 · 64293 Darmstadt - Germany
Telefon + 49 - 6151 90 2016 · Telefax.:+ 49 - 6151 90 2871
www.esa.int





Zukünftiger Ansatz zum Schutz von Produktdaten

Neue Verfahren zum Schutz von Produktdaten müssen immer auch die spezifischen Anforderungen der Anwender erfüllen. Aus diesem Grund arbeiten wir in einem gemeinschaftlichen Produktentwicklungsprozess mit verschiedenen Automobilunternehmen, Forschungsinstituten, ERM- und CAD-Systementwicklern zusammen.

Unsere Forschung konzentriert sich auf zwei Hauptgebiete:

- **Bewertung von aktuellen ERM-Lösungen:** Aktuelle ERM-Lösungen werden entsprechend den Anforderungen der Automobilindustrie bewertet. Bisher wurden verschiedene Tests durchgeführt und deren Ergebnisse als Grundlage für die Weiterentwicklung genutzt: Automobilunternehmen entscheiden mithilfe unserer Ergebnisse, an welchen Schnittstellen und für welche Szenarien die jeweilige ERM-Lösung angewendet wird. ERM- und CAD-Entwickler verbessern mithilfe der Ergebnisse die aktuellen Lösungen, und Wissenschaftler der TU Darmstadt erforschen am CASED verbesserte ERM-Konzepte.
- **Entwicklung von Konzepten zur Verbesserung von ERM-Technologien:** Unser neues ERM-Konzept wird erstmals feingranularen Schutz von CAD-Daten ermöglichen, so dass autorisierte Benutzer ausschließlich auf jeweils für sie relevante Informationen zugreifen können. So soll

die Sicherheit von Firmen-Know-how um ein Vielfaches gesteigert werden. Die neue Methode kombiniert ERM- und Datenfilterungsmethoden und vereint so die Vorteile beider (siehe Abb. 4).

Das gesamte geistige Eigentum in einer CAD-Datei wird entsprechend seiner Art der Wissensinformationen auf feingranulare Weise strukturiert und anschließend durch ERM-Verschlüsselung geschützt. Um Wissensinformationen selbst zu strukturieren, wird die Technik aus der Datenfilterungsmethode verwendet. Diese kann verschiedene Arten von geistigem Eigentum verfolgen und ermitteln.



Reiner Anderl ist Vizepräsident der TU Darmstadt und Leiter des Fachgebiets für Datenverarbeitung in der Konstruktion (DiK) im Fachbereich Maschinenbau. Er ist Principal Investigator des LOEWE-Zentrums CASED.



Joselito Rodrigues Henriques ist wissenschaftlicher Mitarbeiter am Institut für Datenverarbeitung in der Konstruktion und Koordinator des Anwendungslabors am CASED.

Sichere Kommunikation über unsichere Kanäle



Wie können Sie Ihre E-Mails auf Ihren Computer herunterladen, ohne dass ein Dritter die Daten heimlich mitlesen kann? Wie können Sie ihr Online-Banking so gestalten, dass es genauso vertraulich abläuft, wie die Transaktion am Bankschalter? Wie wird gewährleistet, dass Ihre Gebote bei der Online-Auktion verlässlich übertragen werden? Antworten auf diese Fragen bieten Verfahren der modernen Kryptographie, die sichere Kommunikation über unsichere Kanäle ermöglichen.

► *Secure Communication over Insecure Channels*

Can emails be downloaded on your laptop without being read by a third party? Can online banking transactions be processed with the same level of confidentiality as transactions at the bank counter? How is it possible to ensure that online auction bids are transmitted securely and reliably? Cryptography provides answers to all these questions in form of mechanisms that ensure secure communication over insecure channels.

Marc Fischlin, Stefan Katzenbeisser, Mark Manulis •

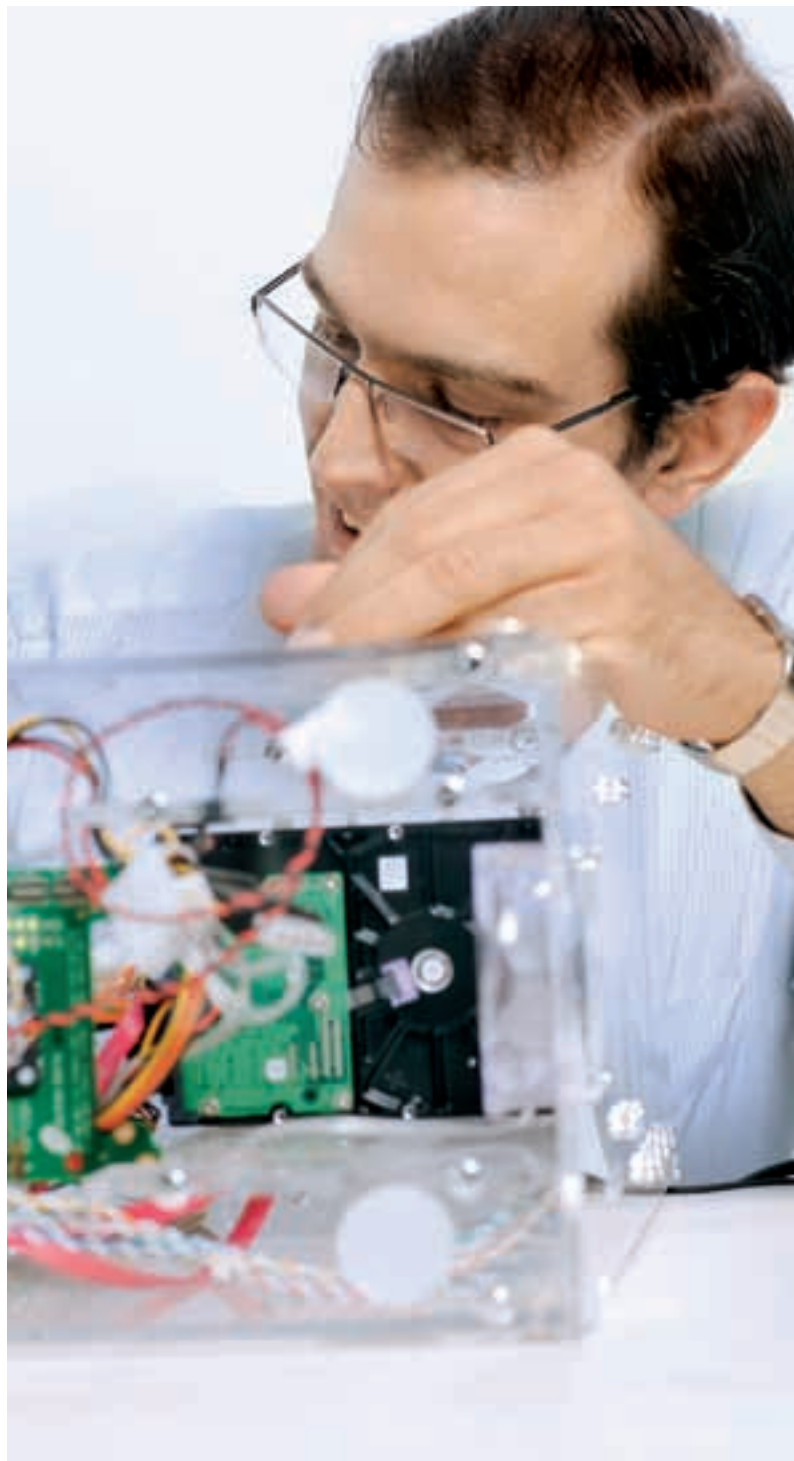
Die moderne Kryptographie stellt vielfältige Verfahren zur Verfügung, die es zwei Kommunikationspartnern – bekannt als Alice und Bob – erlauben, über einen unsicheren Kanal wie das Internet zu kommunizieren, selbst wenn er von einer Angreiferin – genannt Eve – kontrolliert wird. Den grundsätzlichen Lösungsansatz haben Whitfield Diffie und Martin Hellman schon im Jahr 1976 beschrieben (siehe auch Infobox): Alice und Bob einigen sich zunächst über einen unsicheren Kanal auf einen kryptographischen Schlüssel, den Eve nicht aus übertragenen Teilm Informationen errechnen kann.

Dieser Vorgang ist der sogenannte Schlüsseltausch. Alice und Bob verwenden danach diesen Schlüssel, um die eigentliche Kommunikation abzusichern. Da Eve den verwendeten Schlüssel nicht kennt, kann sie die weitere Kommunikation zwischen Alice und Bob nicht mehr abhören. Dieser Ansatz ist heute in zahlreichen Internet-Anwendungen implementiert.





Mark Manulis
(links),
Marc Fischlin
(mitte)
und Stefan
Katzenbeisser
(rechts)



Quantenkryptographie

– die Quantenphysik als Garant für sichere Kommunikation

Die Entwicklung der Quantenmechanik ist eine Erfolgsgeschichte. Dennoch gab es bis vor kurzem keine Anwendung, die tatsächlich auf den ungewöhnlichen Eigenschaften dieser Theorie, wie Komplementarität und Nichtlokalität, beruht. In den letzten Jahren haben jedoch fortgeschrittene experimentelle Methoden und theoretische Modelle die Quanteninformation als eigenes Forschungsgebiet etabliert. Dieses stellt einerseits eine Bedrohung für die immer wichtiger werdende Verschlüsselung von Daten dar, bietet andererseits aber auch eine Lösung für die verursachten Probleme.

► *Quantum Cryptography – Quantum Physics as a Guarantee for Secure Communication*

The development of Quantum Mechanics is a true success story. Until recently, however, there have not been any applications which are actually based on its peculiar properties, namely complementarity and non-locality. But during the last few years more refined experimental methods and theoretical models have established quantum information as an independent field of research. On the one hand quantum information poses a threat to the increasingly-important encryption of data, but on the other hand it provides its own solution.

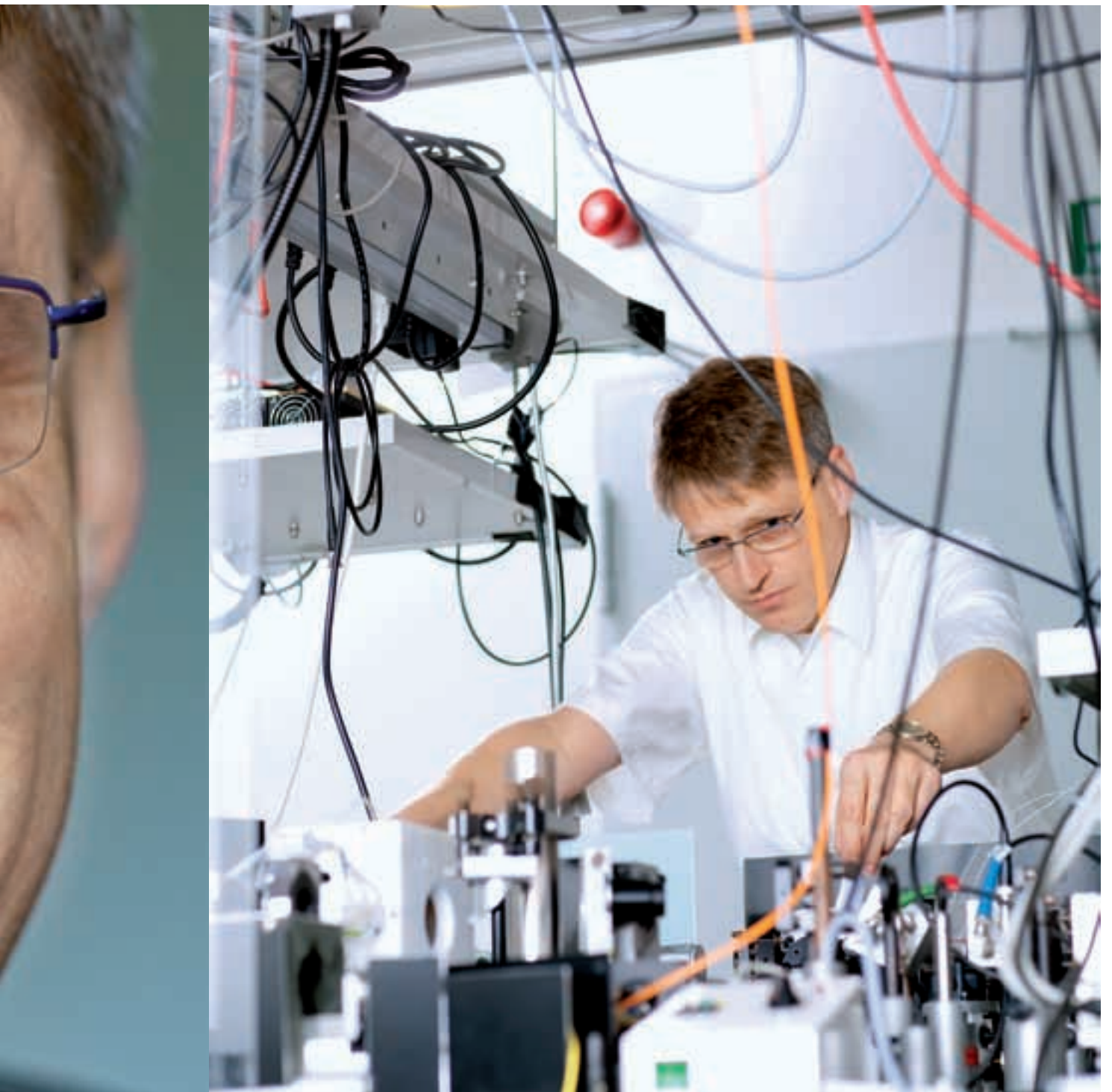
Gernot Alber, Joseph M. Renes, Thomas Walther •

Unbemerkt hat sich die Verschlüsselung von Daten in unseren Alltag eingeschlichen. So werden die Daten, die auf EC- und Kreditkarten gespeichert sind, gegen den unbefugten Zugriff von Dritten durch eine aufwändige Verschlüsselung geschützt. Noch unauffälliger findet die Verschlüsselung bei jedem Onlinebanking-Prozess oder Online-Kauf statt. Nur ein kleines geschlossenes Vorhängeschloss im Fenster des verwendeten Programms kennzeichnet die komplexen Verschlüsselungsmechanismen, die im Computer ablaufen. Die momentan eingesetzten Kryptographieverfahren basieren meist auf sogenannten Public-Key Verfahren. Nach diesen existieren zwei Schlüssel, ein öffentlicher und ein privater, geheimer Schlüssel.

Den öffentlichen Schlüssel kann jeder besitzen und er wird benutzt, um eine Botschaft zu verschlüsseln, während die Entschlüsselung nur durch den privaten, geheimen Schlüssel erfolgen kann und damit nur durch den rechtmäßigen Empfänger der Nachricht. Mathematisch gesehen basiert die Sicherheit dieses Verfahren darauf, dass es leicht ist, mit Hilfe des öffentlichen Schlüssels eine beliebige Nachricht



Thomas Walther





Gernot Alber

zu verschlüsseln, die Entschlüsselung der verschlüsselten Nachricht ohne zusätzliche Kenntnis des privaten, geheimen Schlüssels jedoch sehr zeitaufwändig und mit normalem Computeraufwand daher praktisch unmöglich ist. Das derzeit gängige Public-Key Verfahren ist das RSA-Verfahren, dessen mathematische Grundlage die Primfaktorenzerlegung großer Zahlen ist. Es ist benannt nach seinen Erfindern R. L. Rivest, A. Shamir und L. Adleman. Die Quantenmechanik könnte einerseits eine Bedrohung für dieses Verfahren darstellen, andererseits aber gleichzeitig auch eine Lösung für sichere Kommunikation aufzeigen.

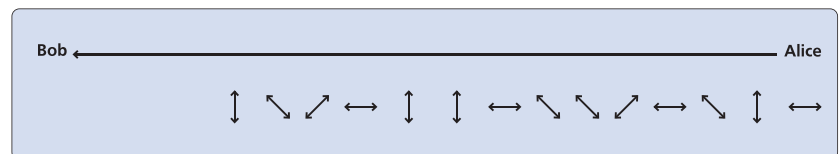
Die Entwicklung der Quantenmechanik begann mit den Entdeckungen Plancks im Jahre 1900, setzte sich über die Erklärung des Photoeffekts

durch Einstein im Jahre 1905 fort und war in den wesentlichen Teilen in den 30er Jahren des vorigen Jahrhunderts abgeschlossen. Nach wie vor gibt die Quantenmechanik Rätsel auf, da sie Vorhersagen macht, die dem Alltagsempfinden zuwider laufen. Sie ist jedoch die vielleicht erfolgreichste Theorie in der Geschichte der Physik. Mit ihrer Hilfe konnten viele Effekte des Mikrokosmos erklärt werden. Immer noch werden durch raffinierter werdende Experimentiertechniken und besseres theoretisches Verständnis neue überraschende Erkenntnisse gewonnen. Praktisch alle Errungenschaften des modernen Lebens basieren letztlich auf der detaillierten Kenntnis quantenmechanischer Vorgänge. Bisher spielen die bizarren Quanteneffekte in Computern oder

Das BB84-Protokoll im Einzelnen

Alice und Bob möchten einen geheimen Schlüssel austauschen, ohne dass Eve den Schlüssel abhören kann. Dies geschieht im BB84 Protokoll durch einzelne Photonen, die zufällig von Alice in einem von vier möglichen Polarisationszuständen zu Bob gesendet werden. Die vier möglichen Polarisierungen sind horizontal und vertikal – diese beiden bilden die +-Basis sowie +45 Grad und -45 Grad polarisiert – letztere bilden die X-Basis. Je ein Zustand jeder Basis wird als „0“ und je einer mit „1“ kodiert. Alice sendet eine große Zahl von einzelnen Photonen in einem der vier Polarisationszustände zu Bob.

Bob entscheidet sich bei der Messung jedes einzelnen Photons zufällig für eine der beiden Basen, + oder X, in denen er seine Messung vornimmt. Das Ergebnis stimmt mit dem von Alice gesendeten Zustand überein, sofern die Basen gleich sind. Andernfalls ist das Ergebnis infolge der Komplementarität der Quantenphysik rein zufällig. Um nun den Schlüssel zu generieren, tauschen Alice und Bob über einen klassischen unsicheren Kanal, zum Beispiel eine Telefonleitung oder das Internet, die verwendeten Basen aus. Stimmen diese überein, werden die entsprechenden Ergebnisse als Teil des Schlüssels verwendet und ansonsten verworfen. Damit festgestellt



Alice	0	0	1	1	0	0	1	0	0	1	1	0	0	1
Bob's Basis	+	+	x	x	+	x	+	+	x	x	+	+	x	+
Bob's Resultat	0	1	1	0	0	0	1	1	0	1	1	1	0	1
Vergleich	✓		✓		✓		✓	✓	✓		✓		✓	
Schlüssel	0	-	1	-	0	-	1	-	0	1	1	-	-	1

werden kann, ob eine dritte Person, Eve, beim Schlüsselaustausch gelauscht hat, werden stichprobenartig einige der Messergebnisse verglichen und dann aus dem Schlüssel entfernt. Treten bei diesem letzten Vergleich mehr Fehler auf als die protokollabhängige Fehlerschwelle zulässt, kann durch Fehlerkorrektur und Privatsphärenverstärkung kein geheimer Schlüssel erzeugt werden, und das Protokoll muss abgebrochen werden. Je nach verwendetem Fehlerkorrektur- und Privatsphärenverstärkungsverfahren liegt diese Fehlerschwelle zwischen 11% und 20%.

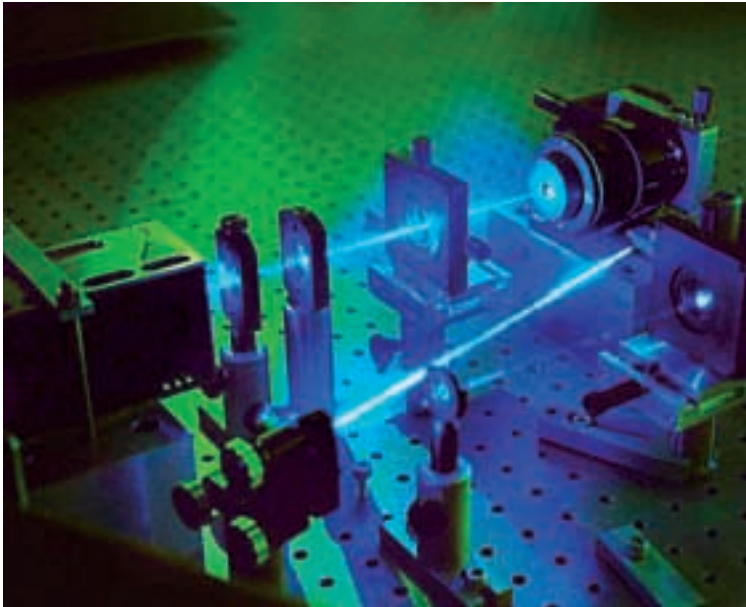
Kodierung	0	1
+Basis	↕	↔
x-Basis	↘	↗

Handys jedoch kaum eine Rolle. Dies könnte sich jetzt erstmals ändern.

Eine noch in der Zukunft liegende Anwendung der Quantenmechanik stellt die Realisierung des Quantencomputers dar. Quantencomputer gehorchen den Gesetzen der Quantenmechanik und könnten deshalb massiv parallel rechnen. So könnten sie zum Beispiel quasi gleichzeitig alle Zahlen auf einmal miteinander multiplizieren. Während dies kaum von praktischem Nutzen sein dürfte, bieten sich Möglichkeiten, die Primfaktorenzerlegung mit einem Quantencomputer wesentlich schneller durchzuführen als dies mit klassischen Computern möglich ist. Somit wäre das oben genannte RSA Verfahren in seiner Sicherheit gefährdet.

Als Reaktion auf diese Gefährdung sind drei Strategien möglich:

1. Die Gefährdung durch den Quantencomputer wird zunächst ignoriert, da die zu schützenden Daten nicht sensibel sind.
2. Man verwendet anstatt des RSA-Verfahrens andere Public-Key-Verfahren, die auf anderen mathematisch schwierigen Problemen basieren, für die der Quantencomputer (bis jetzt noch) keine Bedrohung darstellt.
3. Man verwendet quantenkryptographische Verfahren, die eine sichere Kommunikation auf Basis quantenmechanischer Gesetze ermöglichen. Sie bieten damit eine Sicherheit, die nicht auf mathematischer Komplexität basiert, sondern auf physikalischen Gesetzen. Quantenkrypto-



graphie verwendet im Gegensatz zu den oben genannten Public Key-Varianten eine symmetrische Verschlüsselung, bei der beide Partner denselben zufälligen Schlüssel besitzen. Die Sicherheit quantenkryptographischer Verfahren kann mathematisch bewiesen werden.

Mittels der Quantenkryptographie ist so ein sicherer Informationsaustausch zwischen einer Person A, genannt Alice und einer Person B, genannt Bob, möglich, ohne dass irgendeine dritte Person, genannt Eve, die Kommunikation erfolgreich und unbemerkt abhören kann. Die Sicherheit basiert dabei auf folgenden Grundprinzipien:

1. Schon die klassische Kryptographie zeigt, dass eine Nachricht sicher verschlüsselt werden kann, wenn der verwendete Schlüssel eine absolut zufällige Zeichenfolge ist, genauso lang wie die Botschaft selbst ist und nur einmal verwendet wird. Wichtiger als die kryptographischen Verfahren selbst sind also vielmehr die richtige Wahl des Schlüssels und dessen sichere Übertragung.
2. Ein allgemeiner Quantenzustand lässt sich nicht beliebig kopieren ohne ihn zu verändern – dies ist das sogenannte No-Cloning Theorem.

Institut für Angewandte Physik

Prof. Dr. Gernot Alber
Tel. 06151/16-4802
E-Mail: gernot.alber@physik.tu-darmstadt.de
www.iap.tu-darmstadt.de/tqp/

Dr. Joseph M. Renes
Tel. 06151/16-2381
E-Mail: joerenes@gmail.com
www.iap.tu-darmstadt.de/tqp/grp_jrenes/index.html

Prof. Dr. Thomas Walther
Tel. 06151/16-2182
E-Mail: Thomas.Walther@physik.tu-darmstadt.de
www.iap.tu-darmstadt.de/lqo

Abbildung 1 UV Diodenlaser und optische Komponenten, die im Darmstädter Aufbau genutzt werden, um eine Einphotonenquelle für das BB84 Protokoll aufzubauen.

Für einen sicheren Schlüsselaustausch existieren verschiedene Protokolle. Das historisch erste Protokoll, das BB84-Protokoll, wird im Infokasten schematisch dargestellt. Allen Protokollen gemeinsam ist der Austausch eines geheimen zufälligen Schlüssels durch einzelne Photonen, die mittels verschiedener Verfahren erzeugt werden können. Dies sowie der hocheffiziente Nachweis der Lichtteilchen stellen die größten experimentellen Herausforderungen bei der Quantenkryptographie dar. Ohne die Erfindung des Lasers, die vor ziemlich genau 50 Jahren erfolgte, sowie der Entwicklung geeigneter Halbleitermaterialien wäre beides unmöglich.

Das Besondere an der Quantenschlüsselverteilung ist, dass sich die Präsenz eines Lauschers, Eve, durch Alice und Bob feststellen lässt. Jeder Lauschangriff wird aufgrund des No-Cloning Theorems Spuren hinterlassen und so die von Alice zu Bob gesendeten Photonen verändern. Vergleichen also Alice und Bob nach dem Schlüsselaustausch stichprobenartig einige der Bits des Schlüssels – der echte Schlüssel vermindert sich entsprechend –, muss die festgestellte Fehlerrate unterhalb einer kritischen Schwelle liegen. Andernfalls wird das Protokoll abgebrochen. Liegen die beobachteten Fehler unterhalb dieser kritischen Schwelle, können diese mit Fehlerkorrekturmethode korrigiert werden und die Information, die Eve über den Zufallsschlüssel besitzen könnte, kann mit Hilfe von Privatsphärenverstärkung verschwindend klein gemacht werden.

Die Quantenkryptographie hat ihre Alltagstauglichkeit in bestimmten Situationen bereits bewiesen. So wurden quantenkryptographisch verschlüsselte Banküberweisungen getätigt, Telefonate durch einen zuvor ausgetauschten Quantenschlüssel abgesichert, Wahlergebnisse sicher übertragen, und auch bei der Fußball-WM kam sie im Spielort Durban zum Einsatz. Trotzdem bleiben noch viele Herausforderungen offen, bis sie allumfassend eingesetzt werden kann: Dazu gehört zum Beispiel die Länge der möglichen Übertragungsstrecke. In einer Freistrahübertragung mit Sichtkontakt zwischen Alice und Bob beträgt der Rekord zurzeit 144 km und in optischen Fasern 250 km. Die Übertragungsraten sind bei diesen Entfernungen allerdings sehr gering, so dass ein allgemeiner praktischer Einsatz (noch) unmöglich ist.

Die Quantenkryptographie ist ein sehr spannendes Forschungsthema, das wie in Darmstadt wesentlich durch die enge Verzahnung von Theorie und Experiment lebt. Aktuelle Forschungsthemen sind zum Beispiel die Erhöhung der Übertragungsraten und -distanzen, neue Verfahren zur Fehlerkorrektur und

Adaptive Hardware

für mehr IT-Sicherheit

Hardware, die in ihrer Funktion dynamisch veränderbar ist, ermöglicht heute Lösungen, die mit den bisherigen Mitteln der Informationstechnologie nicht erreicht werden können. Extrem hohe Geschwindigkeiten als auch die Fähigkeit zur nachträglichen Anpassung bieten vielfältige Ansätze für IT-Sicherheitstechnologien. Diese Vorteile können wir für zukünftige Systeme praktisch nutzen.

► *Adaptable Hardware as a Powerful Means to Improve IT Security*

The ability to dynamically change the functionality of hardware modules yields novel technical solutions to many computation problems, which were not achievable before. Inherent high processing speeds as well as the ability to adapt the functionality of a system at any time make this so called reconfiguration technology the premier choice in IT security applications. How can we make use of the unique advantages of adaptable hardware for future systems?

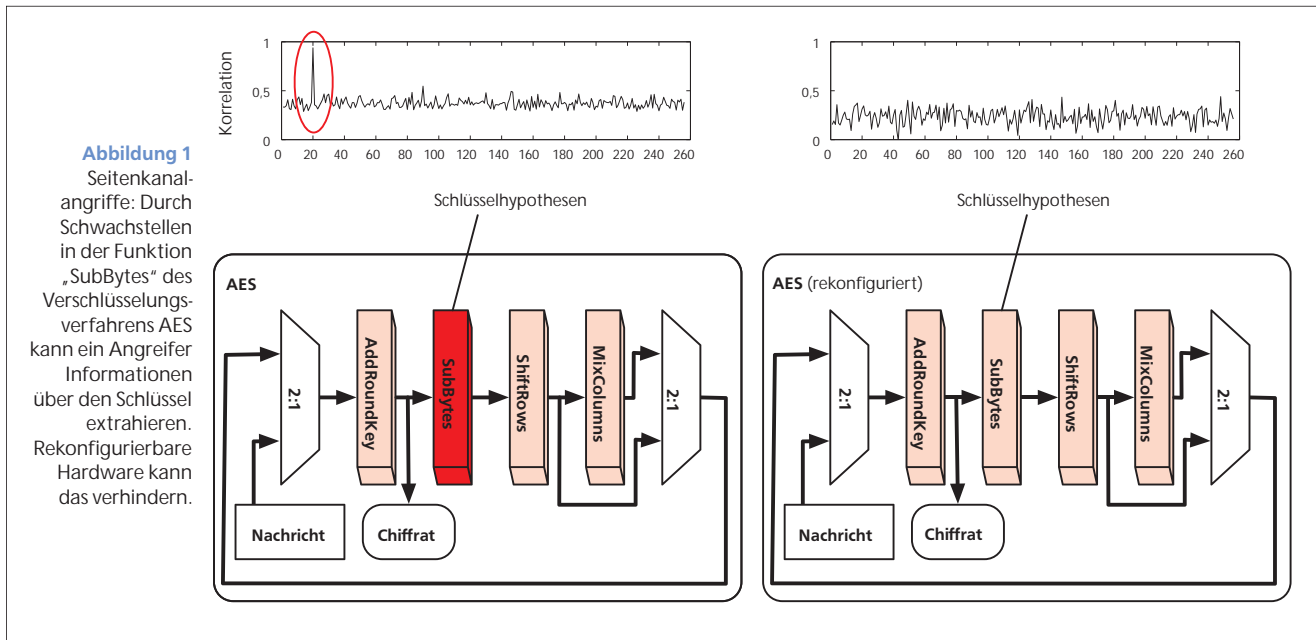
Sorin A. Huss, Andreas Koch, Sascha Mühlbach, Marc Stöttinger • Dank der rasanten Entwicklung der Prozessortechnik in den letzten Jahrzehnten sind wir es gewohnt, dass sich die Leistung von Computern etwa alle zwei Jahre verdoppelt. Allerdings haben technologische Grenzen seit einiger Zeit zu einer Stagnation der Leistung eines einzelnen Prozessors geführt. Ausgeglichen wird dieses Defizit durch die Verwendung von Mehrprozessorsystemen oder durch den Einsatz von speziell für einen Anwendungsbereich zugeschnittener Hardware, die in diesem Bereich deutlich schneller arbeitet als ein generischer Prozessor. Verwendet wird solche Spezialhardware zum Beispiel für die Beschleunigung der Wiedergabe von HD-Videos.

Allerdings ist bei diesem Ansatz für jedes weitere Anwendungsgebiet eine neue spezialisierte Hardware erforderlich, deren Entwicklung und Fertigung sehr aufwendig ist. Eine interessante Alternative sind rekonfigurierbare Hardware-Architekturen, bei denen die Funktionalität der Hardware-Elemente dynamisch umprogrammiert werden kann und nicht bereits durch den Produktionsprozess festgelegt ist. Die am häufigsten verwendete konfigurierbare Architektur ist hierbei das Field Programmable Gate Array (FPGA) (siehe Info-Box).



Andreas Koch





Rekonfigurierbare Architekturen erobern zurzeit aufgrund dieser Vorteile eine Reihe von Anwendungsfeldern, insbesondere auch im Bereich der IT-Sicherheit. Durch die wesentlich höhere Leistungsfähigkeit gegenüber rein softwaregestützten Lösungen können selbst moderne Hochge-

schwindigkeitsnetzwerke vollständig abgesichert werden. Zudem ist es möglich, auf direkte Angriffe auf die Hardware, wie etwa durch Seitenkanal-angriffe, zu reagieren und gefährdete Systeme nachträglich abzusichern. Die folgenden zwei Beispiele aus der Praxis zeigen, wie mittels dieser Tech-

ANZEIGE

Tiefkühl-Pizza *

über die A5 *

Ob bei der Zementherstellung für Beton oder im Stahlwerk, Schenck Process Wäge- und Dosiersysteme sorgen für stabile Brücken.

Käse ist nicht gleich Käse. Schenck Process Dosiertechnik sorgt für die richtige Mischung und so für perfekte Pizzen und auch Pasta ...

nasse Haare *

Bling-Bling *

Damit es so richtig funkelt, braucht es natürlich einen Diamantring. Vom größten Kohlebrocken bis zum kleinsten Diamanten, Schenck Process Siebtechnik ist auch hier immer dabei.

in den Feierabend *

Feierabend! Jetzt nur noch mit dem Zug nach Hause. Oder zur nächsten Party. Diagnosesysteme von Schenck Process sorgen dafür, dass Sie sicher ankommen.

Überall, wo es etwas zu wiegen gibt, steckt Schenck Process dahinter.

Schenck Process GmbH, Pallaswiesenstr. 100, 64293 Darmstadt, Germany, T +49 61 51-15 31 22 39, humanresources@schenckprocess.com, www.schenckprocess.com

*** IBS Heavy**

IBS Light *

*** IBS Mining**

*** IBS Power**

*** IBS Transport Automation**

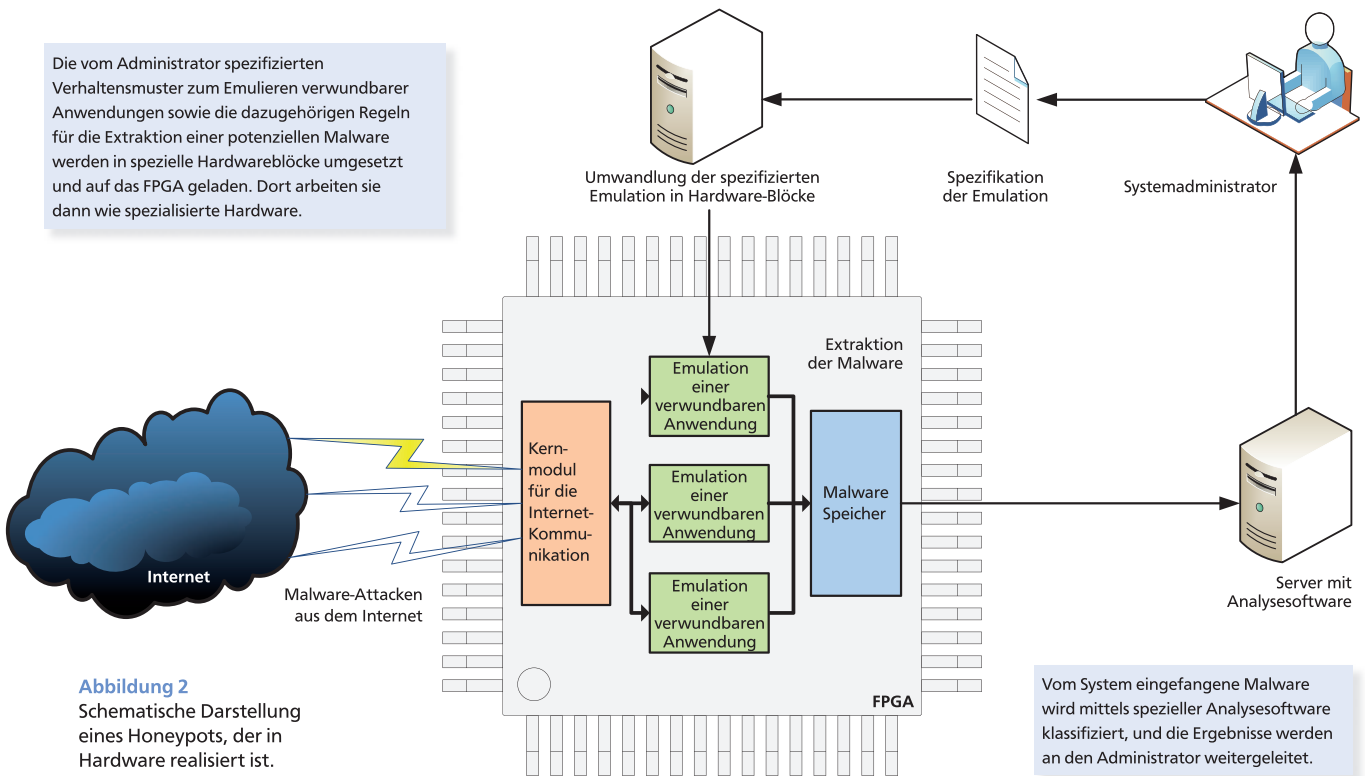


Abbildung 2
Schematische Darstellung eines Honeypots, der in Hardware realisiert ist.

nologie leistungsfähige Plattformen zur Lösung von aktuellen Problemen der IT-Sicherheit geschaffen werden können.

Die Bedrohung durch Schadprogramme, sogenannte Malware, gehört derzeit zu einer der größten Gefahren im Internet. Diese Programme sind oftmals darauf ausgelegt, vertrauliche Informationen zu stehlen oder die Kontrolle über Rechner zu übernehmen. Sie werden über Schwachstellen in Anwendungsprogrammen verbreitet, die zum Beispiel bei der Kommunikation über das Internet ausgenutzt werden.

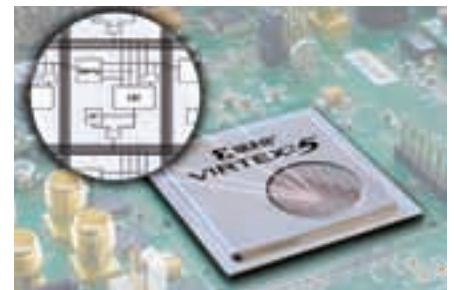
Virens Scanner bieten einen gewissen Schutz vor solchen Bedrohungen, indem sie den Computer regelmäßig nach Verhaltensmustern untersuchen, die auf Schadprogramme hindeuten können. Allerdings entwickelt sich diese Malware kontinuierlich weiter. Es ist daher notwendig, die Erkennungsalgorithmen für bösartige Software ständig zu aktualisieren. Zu diesem Zweck sammeln Wissenschaftler möglichst viele Schadprogramme zur Analyse. Als Quelle hierfür dienen unter anderem spezielle Computersysteme, deren Zweck es ist, automatisch Malware anzulocken. Diese Systeme, sogenannte Honeypots, bilden verwundbare Anwendungsprogramme nach (emulieren sie) und werden ungeschützt im Internet platziert, wo sie von Malware infiziert werden sollen. Der Aufbau solcher größtenteils ungeschützter Systeme birgt jedoch das Risiko, dass diese selber gekapert und für Angriffe auf weitere Maschinen miss-

braucht werden können. Zudem wird eine hohe Rechenleistung benötigt, um möglichst viele Angreifer bedienen zu können und so ein breites Spektrum unterschiedlicher Malware zu erhalten. Unter Berücksichtigung dieser beiden Punkte arbeiten Wissenschaftler des Fachgebiets „Eingebettete Systeme und ihre Anwendungen“ am CASED an

FPGA – Field Programmable Gate Array

Ein typisches FPGA besteht aus mehreren zehntausend frei programmierbaren Verarbeitungselementen, den Logikzellen. Diese sind regelmäßig angeordnet und mittels einer flexibel programmierbaren Struktur miteinander verbunden. Jede Zelle enthält ein 2ⁿ Bit großes RAM, in dem alle logischen Funktionen mit n Eingängen realisierbar sind. Die Funktionswerte werden als Look-Up-Wertetabelle abgespeichert.

Zusätzliche Elemente dienen zur Optimierung von häufig auftretenden Operationen, wie etwa der Addition. Zur Konfiguration eines FPGA werden die Look-Up-Tabellen und die Verbindungsstruktur umprogrammiert. Die aktuelle Konfiguration kann dabei jederzeit überschrieben werden.





einem speziellen Honeypot, der durchgängig in Hardware realisiert ist. Durch die Verwendung von FPGAs können die verschiedenen Anwendungsemulationen flexibel programmiert werden. Trotzdem besteht nicht die Gefahr, dass das System gekapert wird, da Hardware-Strukturen im Gegensatz zu

Fachgebiet Integrierte Schaltungen und Systeme

Prof. Dr.-Ing. Sorin A. Huss
Tel. 06151/16-3980
E-Mail: huss@iss.tu-darmstadt.de, sorin.huss@cased.de

Dipl.-Ing. Marc Stöttinger
Tel. 06151/16-3978
E-Mail: stoettinger@iss.tu-darmstadt.de
www.vlsi.informatik.tu-darmstadt.de
www.cased.de

Fachgebiet Eingebettete Systeme und ihre Anwendungen

Prof. Dr.-Ing. Andreas Koch
Tel. 06151/16-4378
E-Mail: koch@esa.cs.tu-darmstadt.de

Dipl.-Ing. Sascha Mühlbach,
Tel. 06151/16-50182
E-Mail: sascha.muehlbach@cased.de
www.esa.cs.tu-darmstadt.de

Software von außen nur schwer beeinflussbar sind. Zudem kann durch die Ausnutzung von parallelen Rechenoperationen auf dem Chip eine hohe Anzahl von Anfragen gleichzeitig verarbeitet werden. Der Kern des Systems, siehe Abbildung 2, ist eine sehr schnelle Implementierung der Basisprotokolle, die für die Kommunikation im Internet benötigt werden. An diese Protokolle sind die einzelnen Emulationen verwundbarer Anwendungen angeschlossen. Eine Emulation ist immer nur für einen bestimmten Typ von Anfrage (z. B. Internet oder E-Mail) zuständig und emuliert die dort gängigen Schwachstellen. Einkommende Anfragen werden vom Kern analysiert und an die dafür zuständige Emulation weitergereicht. Die Funktionalität der Emulationen wird vom Administrator in einer speziellen Beschreibungssprache definiert und automatisch in eine ausführbare Hardware-Einheit umgesetzt. Die dadurch eingefangene Malware wird gespeichert und kann dann zum Beispiel mit Hilfe von Analyseprogrammen weiterverarbeitet werden. Das System hilft somit, sich ausbreitende Malware auch bei der weiter zunehmenden Geschwindigkeit der Datennetze schnell

Sorin A. Huss

zu erkennen und frühzeitig Gegenmaßnahmen zu ergreifen.

Neben Software-gestützten Angriffen auf Computersysteme können heutzutage jedoch auch direkt die Hardware-Komponenten eines Systems Ziel von Angriffen sein und müssen dementsprechend gesichert werden. Eingebettete Systeme, also in sich abgeschlossene Computersysteme in Miniaturformat, breiten sich vermehrt in allen Lebensbereichen aus. Dadurch verarbeiten sie auch immer mehr persönliche und vertrauliche Informationen. Um rechenintensive Sicherheitsfunktionalitäten wie Verschlüsselungsverfahren in diese Systeme zu integrieren, wird spezialisierte Hardware eingesetzt. Diese ist meist schneller und insbesondere stromsparender als eine Software-gestützte Lösung.

Jedoch stellen spezielle Hardware-Angriffsverfahren wie Seitenkanalangriffe eine Gefahr für die privaten Daten in diesen Systemen dar. Seitenkanalangriffe nutzen das Laufzeitverhalten der implementierten Verschlüsselungsverfahren, um daraus Informationen für einen Angriff zu erhalten. Sehr verbreitet sind auf Leistungsanalysen basierende Angriffe (Power Attacks). Dabei misst der Angreifer die Leistungsaufnahme des Geräts im aktiven Zustand, während das Gerät das korrespondierende Chiffre oder die unverschlüsselte Nachricht verarbeitet. Unter Kenntnis des Verschlüsselungsalgorithmus kann er nun Hypothesen für den im System verwendeten geheimen Teilschlüssel über den datenabhängigen Leistungsverbrauch einer markanten (z. B. leistungsintensiven) Operation im Algorithmus aufstellen. Der Angreifer vergleicht danach die vom Gerät aufgezeichneten Leistungsmessungen mit den Hypothesen durch statistische Methoden. Hierfür wird in der Regel ein Korrelationsverfahren zum Schätzen des Wertes eines Teilschlüssels mit einer hohen Zuverlässigkeit verwendet.

Angreifer können beispielsweise bei dem Verschlüsselungsverfahren AES die Funktion „SubBytes“ ausnutzen, um anhand ihres stark datenabhängigen Leistungsverbrauchs Hypothesen für einen Seitenkanalangriff aufzustellen. Mit Hilfe dieser Hypothesen kann dann mit einem Korrelationsverfahren die wahrscheinlichste Hypothese und damit der richtige Teilschlüssel gefunden werden. (siehe Abbildung 1, links).

Rekonfigurierbare Architekturen bieten hingegen die Möglichkeit, Eigenschaften des Designs nachträglich zu ändern (sollte ein existierendes Gerät anfällig für einen Angriff sein) und sogenannte Verschleierungs- und Maskierungsmaßnahmen in die Schaltung einzubringen. Dies ist einer der Forschungsschwerpunkte der Mitarbeiter im Seitenkanallabor „SCALab“ am CASED.

Bei AES wird dies zum Beispiel durch die Anwendung der Techniken auf die Operation SubBytes oder den gesamten Algorithmus erreicht. Im Ergebnis führt dies zu einem insgesamt niedrigeren und besser balancierten Leistungsverbrauch und erschwert somit den Angriff. Der rechte Teil der Abbildung 1 demonstriert die Auswirkung einer Verschleierungsmaßnahme direkt auf der Funktion SubBytes im Vergleich zum linken Teil.

Im ewigen Wettstreit mit dem Angreifer entwickeln sich sowohl die Angriffe als auch deren Abwehr weiter. Rekonfigurierbare Architekturen bieten hier die Möglichkeit, auch die Hardware (und nicht nur die Software) bestehender Systeme noch nachträglich zu sichern.



Sorin A. Huss ist seit 1990 Professor an der TU Darmstadt und Leiter des Fachgebiets „Integrierte Schaltungen und Systeme“ sowie des CASED-Forschungsbereichs „Sichere Dinge“.



Andreas Koch ist seit 2005 Professor an der TU Darmstadt und leitet das Fachgebiet „Eingebettete Systeme und ihre Anwendungen“. Er ist an den LOEWE-Zentren CASED und AdRIA beteiligt.



Sascha Mühlbach arbeitet seit 2009 als Doktorand im Themenbereich „Sicherheit in Hochgeschwindigkeitsnetzen“ am Center for Advanced Security Research Darmstadt.



Marc Stöttinger arbeitet auf einer DFG-geförderten Forschungsstelle am Fachgebiet „Integrierte Schaltungen und Systeme“ der TU Darmstadt und ist assoziiertes Mitglied am CASED.

Physikalische

Fingerabdrücke gegen Produkt-Piraterie

Produkt-Piraterie stellt ein schwerwiegendes und bisher ungelöstes Problem der heutigen Zeit dar und verursacht wirtschaftliche Schäden in Milliardenhöhe. Existierende technische Lösungsansätze weisen unterschiedliche Schwächen auf, beispielsweise haben sie nur eine begrenzte Anwendbarkeit oder verfehlen die geforderten Sicherheitsziele. Einen vollständig neuen Ansatz stellen Physikalisch unklonbare Funktionen – kurz PUFs – dar. Hierbei werden die bei Herstellungsprozessen unvermeidbaren physikalischen Variationen ausgenutzt, um unter anderem ein physikalisches Pendant zum biometrischen Fingerabdruck zu erzeugen.

► *Using physical fingerprints against product piracy*

Today, product piracy represents a severe and so far unsolved problem, causing commercial damages going into the billions. Existing technical solutions have different drawbacks, e.g., being not universally applicable or missing the required security goals. A completely new approach is the use of Physically Unclonable Functions – short PUFs. Hereby unavoidable physical variations of manufacturing processes are exploited, e.g., for creating a physical variant of biometric fingerprints.

Frederik Armknecht, Ahmad-Reza Sadeghi •

„Besser gut kopiert als schlecht erfunden“ heißt eine bekannte Redewendung. Im Kontext von Produktpiraterie nimmt dies jedoch bedrohliche Ausmaße an. Unter Produktpiraterie versteht man das illegale Geschäft mit Imitaten. Diese werden mit dem Ziel hergestellt, einer Originalware zum Verwechseln ähnlich zu sein, können aber weit unter dem Originalpreis angeboten werden. Die Problematik betrifft nahezu jede Produktgruppe, beispielsweise Bekleidung, Fahr- und Flugzeugteile, Consumer Electronics, Steuergeräte in Anlagen sowie Medikamente und Software.

Dabei werden Markenrechte oder wettbewerbsrechtliche Vorschriften verletzt und immense wirtschaftliche Schäden verursacht. Schätzungen zufolge verursachen diese illegalen Geschäfte jährlich einen wirtschaftlichen Schaden von etwa 600–1200 Mrd. US-Dollar (ca. 10 % des Welt Handels), davon allein 30 Mrd. Euro in Deutschland, und kosten jährlich weltweit 750.000 Arbeitsplätze (davon 70.000 in Deutschland). Selbst wenn es möglich wäre, Waren von minderer Qualität einfach zu erkennen und aus dem Handel zu



Ahmad-Reza Sadeghi

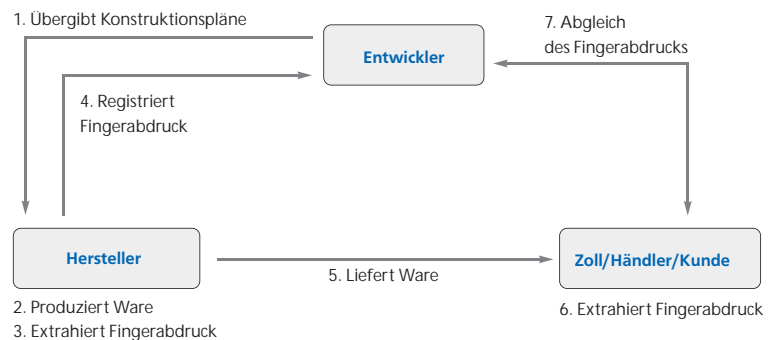


nehmen, wäre die Gefahr nicht gebannt. Ein verwandtes Problem, welches vor allem die Chip-Produktion betrifft, ist die unautorisierte Überproduktion von Waren und deren illegaler Verkauf. Hierbei wird an den Originalproduktionsstätten vom Hersteller, die zumeist in kosteneffektiven und lohnschwachen Ländern liegen, unbemerkt zusätzliche Ware produziert und diese ohne sein Wissen verkauft.

Produktpiraterie hat ernsthafte wirtschaftliche und politische Konsequenzen. Da sie durch gesetzliche Maßnahmen allein nicht zu verhindern ist, wird verstärkt nach effektiven und effizienten technischen Gegenmaßnahmen gesucht. Die existierenden Lösungen weisen jedoch unterschiedliche Schwächen auf: Sie sind entweder zu aufwändig und somit für viele kommerzielle Produkte nicht geeignet, erreichen nicht die angestrebten Sicherheitsziele oder sie sind stark produktabhängig und daher nicht allgemein einsetzbar. Insbesondere zeigt das Problem der Überproduktion deutlich, dass es nicht ausreicht, den Herstellungsort eines Produktes feststellen zu können. Idealerweise sollten die Produkte selbst eindeutig identifizierbar und wieder zu erkennen sein.

Physikalische Fingerabdrücke

Hier bietet die Biometrie Inspiration: Genau wie Menschen anhand ihres biologischen Fingerabdrucks identifiziert werden können, werden eine eindeutige Identifizierung der Ware mittels eines physikalischen Fingerabdruckes angestrebt. Basierend auf solchen physikalischen Fingerabdrücken sieht eine momentan industriell angewandte Lösung wie folgt aus: Sobald die Ware produziert wurde, aber noch bevor sie in den Handel gelangt, wird deren physikalischer Fingerabdruck beim Hersteller registriert. Wenn dann später eine beteiligte Instanz, z.B. ein Händler oder Zöllner, die Rechtmäßigkeit einer erhaltenen Ware überprüfen möchte, wird zunächst ihr physikalischer Fingerabdruck bestimmt und anschließend beim Hersteller erfragt. Sollte der Fingerabdruck nicht beim Hersteller registriert sein, dann bedeutet dies, dass die Ware entweder eine Fälschung ist oder im Rahmen einer Überproduktion erzeugt wurde (siehe Abbildung 1). Da bei der Überprüfung der Fingerabdrücke nur digitale Daten ausgetauscht werden müssen, kann man auf etab-



lierte kryptographische Verfahren wie SSL zurückgreifen, um diese Kommunikation abzusichern.

Physikalisch unklonbare Funktionen

Wie kann man nun geeignete physikalische Fingerabdrücke erhalten? Ähnlich zum menschlichen Fingerabdruck sollten physikalische Fingerabdrücke effizient verifizierbar, eindeutig und fälschungssicher sein. Weitere wichtige Eigenschaften sind, je nach Anwendung, geringe Größe und Herstellungskosten, effiziente Integration und damit weite Einsetzbarkeit der technischen Lösung. Eine Antwort auf die Frage bietet eine neuartige Technologie: Physikalisch unklonbare Funktionen (PUFs). Vereinfacht gesagt ist eine PUF ein physikalisches Gerät, bei dem es möglich ist, Eingaben zu stellen und Ausgaben zu erhalten. Der wesentliche Aspekt hierbei ist, dass das Eingabe-Ausgabe-Verhalten hochgradig von den physikalischen Eigenschaften des Gerätes abhängig ist. Diese wiederum sind weder planbar noch reproduzierbar.

Ein Beispiel sind die sogenannten optischen PUFs. Eine optische PUF besteht aus einem transparenten Material, das mit winzigen lichtstreuenden Partikeln durchsetzt ist, die während des Herstellungsprozesses beigemischt werden. Wenn ein Laserstrahl

Abbildung 1

Technischer Ansatz zum Schutz vor Produktfälschungen und Überproduktion basierend auf PUFs

Institut für Mathematik und Informatik an der Universität Mannheim

Prof. Dr. Frederik Armknecht

Tel. 0621/1812483

E-Mail: armknecht@informatik.uni-mannheim.de

<http://th.informatik.uni-mannheim.de/>

Fachgebiet Systemsicherheit der TU Darmstadt

Prof. Dr.-Ing. Ahmad-Reza Sadeghi

E-Mail: ahmad.sadeghi@cased.de

www.trust.rub.de/

Abbildung 3
Integration der PUF
in die Chiffre

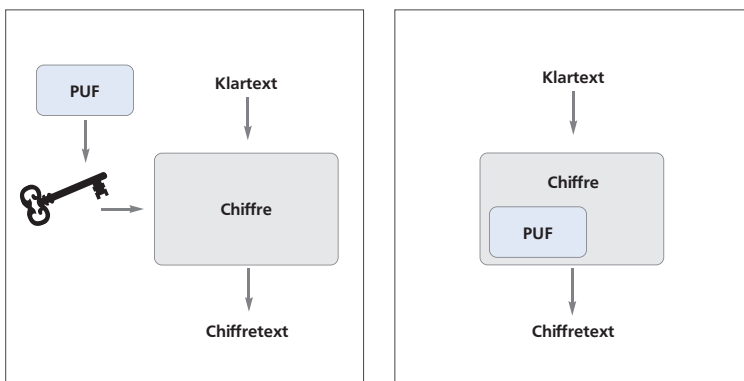


Abbildung 2
PUF als sicherer
Schlüsselspeicher

auf das Material trifft, wird dieser partiell gestreut, so dass der Strahl ein Fleckenmuster wirft. Da dieses Muster durch die Positionen der Partikel bestimmt wird und die Interaktion zwischen dem Laser und den Partikeln sehr komplex ist, ist das Muster zufällig und einzigartig. Insbesondere ist es praktisch unmöglich, eine optische PUF so zu duplizieren, dass das Duplikat das gleiche Fleckenmuster wie das Original erzeugt. Die PUF ist somit unklonbar.

Ein weiteres Beispiel ist die SRAM-PUF, die bereits industriell implementiert wird. SRAM steht für: Static Random Access Memory (Statisches RAM). Hierbei werden gewöhnliche SRAM-Bausteine verwendet, die jedoch direkt nach dem Einschalten ausgelesen werden, also noch bevor sie initialisiert wurden oder Werte gespeichert haben. Ausführliche Experimente haben gezeigt, dass diese Werte von SRAM-Baustein zu SRAM-Baustein variieren und bei der Produktion nicht beeinflusst werden können.

Inzwischen gibt es verschiedene Vorschläge für PUF-Konstruktionen. Allen gemeinsam ist, dass ihr Verhalten stark durch unvermeidbare natürliche physikalische Variationen des Herstellungsprozesses bestimmt wird. Ein wesentlicher Vorteil hierbei ist, dass die ausgenutzten physikalischen Phänomene nicht künstlich erzeugt oder bei der Herstellung speziell berücksichtigt werden müssen. Dies ermöglicht einerseits eine vergleichsweise effiziente und kostengünstige Herstellung und erlaubt andererseits eine Vielzahl von unterschiedlichen PUF-Typen.

Die Einsatzmöglichkeiten von PUFs gehen weit über die oben genannten Anwendungsfelder hinaus. Ein weiteres Anwendungsbeispiel ist der Schutz von Software. Hierbei wird der zu schützende Code mit einem durch die PUF generierten

Schlüssel verschlüsselt. Dadurch kann dieser nur auf der vorgesehenen Anwenderplattform entschlüsselt werden, in welche die PUF eingebettet ist (siehe Abbildung 2). Ein weiteres Beispiel ist ein von uns entwickelter Verschlüsselungsalgorithmus, in dem PUFs nicht mehr nur als Schlüssellieferant verwendet werden, sondern direkt in den Ver- und Entschlüsselungsprozess integriert sind (siehe Abbildung 3). Für diese Konstruktion kann man die Sicherheit sowohl gegen gewisse algorithmische als auch physikalische Angriffe beweisen, falls die eingesetzten PUFs bestimmte Eigenschaften erfüllen. Im Rahmen des EU-Projektes UNIQUE erforschen und entwickeln wir mit Partnern aus der Industrie und dem akademischen Umfeld neue PUF-basierte Lösungen und Konzepte und streben deren prototypische Implementierung an.

PUFs sind sowohl von hoher wissenschaftlicher als auch industrieller Relevanz. Seit PUFs 2002 erstmals öffentlich in einer Doktorarbeit am Massachusetts Institute of Technology (MIT) diskutiert wurden, haben sie sich zu einem vielbeachteten Forschungsthema entwickelt. Das belegen eindrucksvoll weit über 70 Publikationen in teils sehr namhaften Journalen wie „Science“ und mehrere Workshops und Seminare zum Thema PUF. PUFs sind aber nicht nur aus akademischer Sicht interessant, sondern werden, wie bereits erwähnt, schon heute industriell eingesetzt. Als Beispiele seien hier die Firmen Intrinsic ID, eine Auskopplung von Philips, und Verayo, eine Ausgründung des MIT, genannt.

PUFs stellen somit ein hochaktuelles und wichtiges Forschungsgebiet dar und gehören zu den Schlüsseltechnologien der Zukunft, welche die Sicherheit in vielen Anwendungsbereichen verbessern können.



Frederik Armknecht ist Juniorprofessor für Kryptographie an der Universität Mannheim.



Ahmad-Reza Sadeghi ist seit Oktober 2010 Professor am Fachbereich Informatik der Technischen Universität Darmstadt und leitet das Fachgebiet Systemsicherheit. Zudem ist er Principal Investigator des LOEWE-Zentrums CASED.

IT-Forensik

– Technologie für Datendetektive

Finden und Auswerten digitaler Spuren verbotener Aktivitäten kann IT-Forensiker vor große Probleme stellen. Wachsende Datenmengen und Spuren verbotener Aktivitäten, die sich auf den ersten Blick nicht von Spuren erlaubter Aktivitäten unterscheiden, lassen die praktische IT-forensische Arbeit zu einer Suche nach der Nadel im Heuhaufen werden. Am CASED entwickelt das Fraunhofer SIT Lösungen, um die Suche und Analyse digitaler Spuren effektiver und effizienter zu machen. Dies erfordert Technologiewissen in unterschiedlichen Bereichen wie Multimedia, Dateisysteme, Data Mining.

► IT Forensics – Technology for Data Detectives

Detection and analysis of digital traces for elucidating forbidden activities that involve IT systems can pose severe problems for IT forensic investigators. Increasing amounts of data and traces of illegal activities that, from a technical perspective, do not differ from traces of day-to-day work make IT forensic investigation often similar to looking for a needle in a haystack. At CASED researchers from Fraunhofer SIT develop solutions that make search and analysis of digital traces more effective and efficient. This requires knowledge in several areas, e.g., multimedia, file systems, data mining.

Martin Steinebach, Markus Schneider, Michael Waidner • Die Forensik umfasst Methoden, die zur Aufklärung und Rekonstruktion von Tathergängen dienen. Hierzu werden Spuren gesucht, untersucht und ausgewertet. Die Ergebnisse der Methoden dienen dazu, Ermittlungshypothesen

Robuste Hashfunktionen

In der Multimediasicherheit werden Alternativen zu den kryptographischen Hashfunktionen entwickelt, die nicht die binäre Gleichheit der Datei zur Erkennung nutzen, sondern die menschliche Wahrnehmung als Ausgangspunkt sehen. Dabei ist das Ziel, verschiedene Ausprägungen eines Werkes, z. B. eines Bildes, welches mit verschiedenen Stärken durch JPEG komprimiert wurde, als gleich zu identifizieren. Andere Werke sollen aber unabhängig von ihrer Ähnlichkeit als nicht gleich erkannt werden. Da diese Funktionen ähnlich wie kryptographische Hashfunktionen eingesetzt werden, aber im Gegensatz zu diesen robust gegen akzeptable Veränderungen sind, werden solche Funktionen robuste Hashfunktionen genannt.

zu unterstützen oder zu widerlegen. Die IT-Forensik umfasst den Teil der Forensik, in der digitale Spuren behandelt werden, die beispielsweise durch den unrechtmäßigen Einsatz von IT-Systemen entstehen, wie Logdaten. Zur IT-forensischen Untersuchung digitaler Spuren sind geeignete Software-Werkzeuge erforderlich. Die IT-Forensik ist nicht mit der computergestützten Forensik zu verwechseln, bei der mittels Computern auch physische Spuren untersucht werden können, z. B. Fingerabdrücke.

IT-Forensik und IT-Sicherheit ergänzen sich beide in sehr sinnvoller Weise, um die Interessen von rechtmäßigen Nutzern bezüglich ihrer Daten oder IT-Systeme zu schützen. Da diese Interessen in der Praxis nicht immer durch Methoden der IT-Sicherheit effektiv geschützt werden können, braucht man Lösungen, um unrechtmäßige Handlungen in IT-Systemen aufklären zu können und dem Geschädigten zu seinem Recht zu verhelfen. In der Praxis kann man nicht erwarten, dass IT-Systeme gegen jeden denkbaren Missbrauch geschützt sind, zum Beispiel wegen Sicherheitslücken durch Implementierungsfehler oder durch Fehlkonfigurationen.

So wie für die klassische Forensik beispielsweise mit der Ballistik und der Gentechnik viele unterschiedliche Expertisen notwendig sind, sind auch für die IT-Forensik verschiedene Kompetenzen relevant. Als Beispiele hierfür sind etwa die Technologiebereiche Multimedia, Netzwerke, Email, grafische Datenverarbeitung, Datenbanksysteme, digitale Signalverarbeitung, Data Mining, Speichermedien und Dateisysteme zu nennen.

Zur Verdeutlichung der Relevanz der IT-Forensik sei auf reale Vorfälle verwiesen: Laut Bundeskriminalamt (BKA) wurden 2009 in Deutschland 50.254 Fälle von IT-Kriminalität im engeren Sinn registriert, 2008 wurde in bereits mehr als jedem fünften Fall von Wirtschaftskriminalität das Internet benutzt. Die Gesamtschadenssumme betrug 2008 in Deutschland 3,34 Mrd. Euro. Weitere Herausforderungen ergeben sich durch illegale digitale Inhalte (Kinderpornographie, Gewaltvideos), deren Erstellung und Verbreitung heute technisch sehr einfach möglich und kaum zu verhindern sind.

Hat eine kriminelle Handlung stattgefunden, dann besteht die Aufgabe des IT-Forensikers darin, geeignete Datenquellen zu identifizieren, diese si-

Michael Waidner



herzustellen und zur Rekonstruktion des Tathergangs oder zur Beweisführung Datenspuren zu finden. IT-Forensiker werden jedoch auch aktiv, wenn keine konkreten Hinweise auf verbotene Handlungen vorliegen, zum Beispiel bei routinemäßigen Überprüfungen von Datenbeständen in Unternehmen auf Fälle von Wirtschaftskriminalität. Hierbei ist dem IT-Forensiker bei seiner Arbeit oft nicht klar, wonach genau er suchen soll.

Bei solchen Suchen werden unter anderem statistische Tests eingesetzt, durch die Auffälligkeiten erkannt werden sollen.

Die umfangreichen Mengen an Daten, die bei der Spurensuche zu berücksichtigen sind, treiben die Untersuchungskosten in die Höhe und verlangen nach geeigneten IT-Lösungen. Das Problem bei der automatisierten Herangehensweise besteht jedoch darin, dass Spuren übersehen werden können

Abbildung 1

Digitale Bildforensik kann Unregelmäßigkeiten an Bildmaterial erkennen. So wurde das Original links verändert, indem der Golfball mit einem Kopierstempel mit Rasen übermalt und so gelöscht wurde. Das Ergebnis ist in der Mitte zu sehen. Ein forensisches Verfahren macht sichtbar, dass zwei Bereiche des Rasens identisch sind und weist so auf die Manipulation hin.



(False Negatives) oder zu viele Spuren gefunden werden, die sich als völlig harmlos herausstellen (False Positives). Dies wird in einigen Fällen dadurch erschwert, dass für verbotene Handlungen, die auf Missbrauch von Rechten in IT-Systemen basieren, aus technischer Sicht die gleichen Schrittabfolgen anfallen, wie sie von derselben Person viele Male für unkritische oder erwünschte Handlungen ausgeführt werden.

Im Folgenden werden einige Arbeitsgebiete der IT-Forensik, in denen Fraunhofer SIT am CASED aktiv ist, exemplarisch betrachtet.

Multimedia-Forensik: Erkennung verbotener Inhalte

Im Rahmen der forensischen Untersuchung von Datenbeständen wird unter anderem nach illegalem Bildmaterial gesucht. Hierbei handelt es sich in erster Linie um Kinderpornographie. Die Identifizierung kann auf Sichtung oder auf kryptographischen Hashverfahren beruhen, welche den Hashwert eines Bildes berechnen und diesen mit in einer Datenbank gespeicherten Hashwerten vergleichen. Ein Hashwert ist eine Zeichenfolge, die als eine Art Fingerabdruck für eine Datenmenge berechnet werden kann. Bei kryptographischen Hashverfahren besteht aber immer das Risiko eines Nicht-Identifizierens von entsprechendem Material. Dies ist immer dann der Fall, wenn Dateien nicht identisch kopiert werden, sondern beispielsweise Formatwandlungen unterlaufen. Am CASED werden sogenannte robuste Hashverfahren auf ihre Eignung hin zum automatischen Erkennen von Bildmaterial in forensischen Untersuchungen geprüft.

Kamera-Forensik: Erkennung von Datenquellen

Ein Großteil aller Fotos wird heute mit digitalen Kameras erstellt. Das gilt beispielsweise für Gewaltvideos, die mit Handys aufgezeichnet werden, oder für Kinderpornographie. Dieser Umstand kann helfen, Täter zu überführen, indem Kameras im Besitz der Täter mit aufgefundenem Material in Verbindung gebracht werden. Dies wird durch die Kamera-Forensik ermöglicht. Diese errechnet eine Art Fingerabdruck der Kamera, indem eine Serie von Bildern hinsichtlich eines für die Kamera individuellen Eigenrauschens untersucht wird, welches durch Fertigungsungenauigkeiten des bild erzeugenden CCD Chips bei seiner Herstellung bedingt ist. Dieser Fingerabdruck kann dann als Quellennachweis zu einer Kamera dienen – sogar nach verlustbehafteter Kompression oder dem Ausdrucken und Einscannen.

Test IT-forensischer Werkzeuge

Mit der technologischen Weiterentwicklung ergeben sich immer wieder neue Anforderungen an IT-forensische Methoden und Werkzeuge. Deren Leistungsfähigkeit hängt oftmals von besonderen Rahmenbedingungen ab, unter denen sie eingesetzt werden. Entwickler haben heute oft keine Realdaten, anhand derer sie ihre Ergebnisse testen können. Insbesondere ist es Anwendern und Entwicklern häufig nicht klar, wie sich ihre Werkzeuge unter besonderen Bedingungen verhalten. Deshalb ist es wichtig, die Leistungsfähigkeit der Werkzeuge unter gewünschten Bedingungen testen zu können. Fraunhofer SIT hat mit 3LSPG ein Verfahren entwickelt, mit dem IT-forensische Werkzeuge für gegebene Bedingungen mittels synthetisch erzeugter Datenbestände getestet werden können.

Verbesserung IT-forensischer Werkzeuge

Mit diesen Tests ist es möglich, bestehende IT-forensische Methoden zu untersuchen und sie allgemein oder für bestimmte Bedingungen zu verbessern. So liefert die Benford-Analyse, eine IT-forensische Standardmethode, unter bestimmten Bedingungen (z.B. bei Buchungsgrenzen durch Zugriffsbeschränkung) wegen zu vieler False Positives keine brauchbaren Ergebnisse. Mit seinem Beitrag zur modellgestützten digitalen Analyse ist es Fraunhofer SIT gelungen, die Idee der Benford-Analyse weiter zu entwickeln und zu verbessern, indem von der

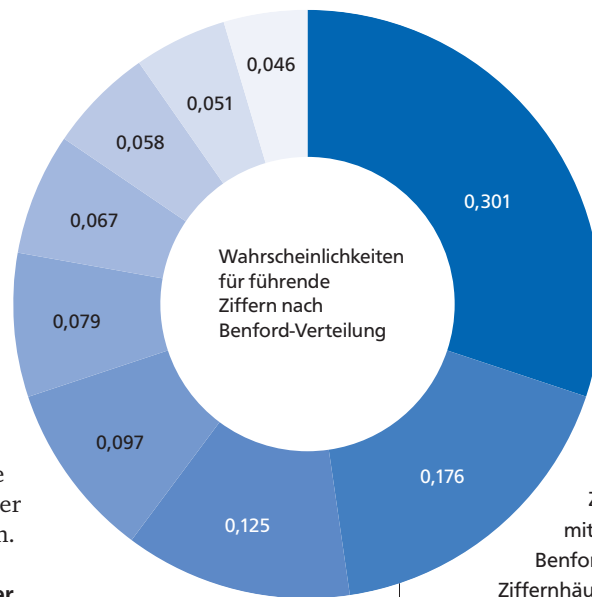
Fraunhofer-Institut für Sichere Informationstechnologie (SIT)

Dr.-Ing. Martin Steinebach
Tel. 06151/869-349
E-Mail: martin.steinebach@sit.fraunhofer.de

Dr.-Ing. Markus Schneider
Tel. 06151/869-337
E-Mail: markus.schneider@sit.fraunhofer.de
www.sit.fraunhofer.de

Fachgebiet für Sicherheit in der Informationstechnik

TU Darmstadt / Fraunhofer-Institut für Sichere Informationstechnologie (SIT)
Prof. Dr. Michael Waidner
Tel. 06151/869-250
E-Mail: waidner@sit.fraunhofer.de
www.sit.fraunhofer.de



Führende Ziffern

- 1 ■ 2 ■ 3
- 4 ■ 5 ■ 6
- 7 ■ 8 ■ 9

Benfords Gesetz

Dieses Gesetz basiert auf der Beobachtung von S. Newcomb (1881) und F. Benford (1934), dass führende Ziffern in vielen Zahlenlisten nicht gleichverteilt sind. Zahlen mit niedrigerer führender Ziffer treten in vielen Listen öfter auf als Zahlen mit höherer führender Ziffer. Daraus wurde die Benford-Analyse entwickelt: Weichen gemessene Ziffernhäufigkeiten zu stark von der Benford-Verteilung ab, dann ist dies ein Indiz für eine Unregelmäßigkeit.

Benford-Verteilung abweichende und auf die konkreten Bedingungen angepasste Verteilungen verwendet werden. Damit können IT-Forensiker ihre Untersuchungen effektiver und effizienter durchführen.

Entwicklung rechtssicherer Analysemethoden

Zur Entdeckung von Tätern sind oftmals für Plausibilitätschecks, Datenabgleiche oder Anomalie-Erkennung Analysen großer Datenbestände notwendig, bei denen Daten vieler Personen verarbeitet werden. Hier kann die IT-Forensik leicht in Konflikt mit dem Datenschutz geraten (z.B. Datenskandal bei der Deutschen Bahn AG 2009). Zur rechtskonformen und leistungsfähigen IT-forensischen Untersuchung sind somit geeignete Verfahren erforderlich.

Es existieren große Herausforderungen bei der Bekämpfung digitaler Kriminalität. Die IT-Forensik kann hier bei der Bewältigung wichtige Hilfsmittel stellen. Eine Herausforderung besteht in der Entwicklung relevanter neuer Lösungen und in dem Transfer von wissenschaftlichem Beitrag zur praktischen Anwendung. Dies ist am CASED eine der Aufgaben des Fraunhofer SIT.



Martin Steinebach leitet am Fraunhofer SIT den Bereich Information Assurance, der sich unter anderem mit IT Forensik und Multimedia Security beschäftigt. Er ist zudem Principal Investigator des LOEWE-Zentrums CASED.



Markus Schneider koordiniert die CASED-Aktivitäten des Fraunhofer SIT und war am Aufbau der IT-Forensik-Gruppe des Fraunhofer SIT beteiligt.



Michael Waidner ist seit 2010 Professor für Sicherheit in der Informationstechnik an der TU Darmstadt und zugleich Leiter des Fraunhofer SIT am Standort Darmstadt. Er ist zudem stellvertretender Direktor des LOEWE-Zentrums CASED.

—ANZEIGE

Die perfekte Location für erfolgreiche Seminare und Workshops.

Tel +49 (0)69 696 13 9100
www.lufthansa-seeheim.de

Lufthansa Seeheim

Wolken und Datenspuren

Die interdisziplinäre Forschung des Centers for Advanced Security Research (CASED) in Kooperation mit dem Forschungszentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel hat vielfältige Bezüge zum Recht. Das IT-Recht, insbesondere das Datenschutzrecht, hat maßgeblichen Einfluss auf IT-Sicherheitslösungen. Rechtliche Forschungsschwerpunkte sind die zukunftssträchtigen Forschungsgebiete "Cloud Computing" und "IT-Forensik" und deren rechtsgemäße Gestaltung unter Beachtung der grundgesetzlichen Vorgaben und der Rechtsprechung des Bundesverfassungsgerichts.

► *Clouds and digital paper trails*

The interdisciplinary research conducted at the Center for Advanced Security Research (CASED) in cooperation with the Research Center for Information Technology Design (ITeG) at the University of Kassel bears multiple relations with law. IT law, especially data protection law, has significant impact on IT security solutions. Legal research emphasis lies on the innovative areas of „cloud computing“ and „IT forensics“. It focuses on legally compliant design of these technologies by respecting constitutional requirements as well as the jurisprudence of Germany's constitutional court, the Bundesverfassungsgericht.

Alexander Roßnagel, Dennis Heinson, Mark Bedner • Sicherheitslösungen müssen Rechtsgüter schützen und ihrerseits rechtsgemäß sein. Rechtswissenschaft kann auf zwei Wegen dazu beitragen, dieses Ziel zu erreichen. Zum einen kann sie Vorschläge erarbeiten, wie Sicherheitslösungen nach rechtlichen Kriterien technisch und organisatorisch gestaltet werden können. Zum anderen kann sie die rechtlichen Vorgaben für Sicherheitslösungen da-

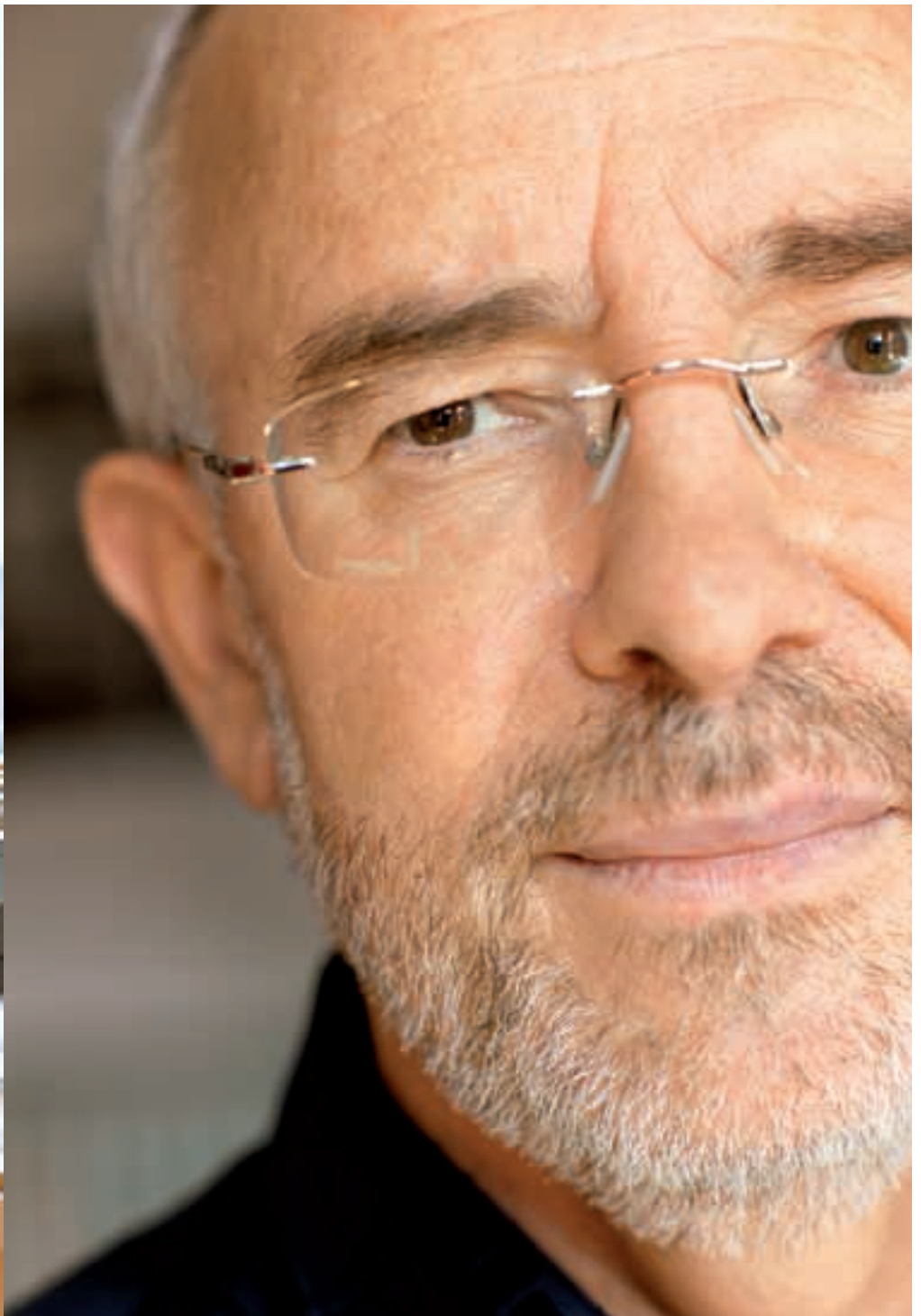
Center for Advanced Security Research Darmstadt
ITeG Universität Kassel
Prof. Dr. Alexander Roßnagel
Tel. 0561/804-2223
E-Mail: a.rossnagel@uni-kassel.de
www.uni-kassel.de/fb7/oeff_recht/

ITeG Universität Kassel
Dennis Heinson, LL.M. (UCLA)
Tel. 0561/804-6080
E-Mail: dennis.heinson@cased.de
www.uni-kassel.de/fb7/provet/heinson/

ITeG Universität Kassel
Ass. iur. Mark Bedner, LL.M.
Tel. 0561/804-6091
E-Mail: mark.bedner@cased.de
www.uni-kassel.de/fb7/provet/bedner/



Alexander Roßnagel



raufhin untersuchen, ob sie änderungs- oder ergänzungsbedürftig sind und in diesem Fall Vorschläge zu ihrer Rechtsfortbildung durch Rechtsprechung und Gesetzgebung erarbeiten. Wie dies in CASED in interdisziplinärer Kooperation mit der Informatik möglich ist, soll an zwei Beispielen erläutert werden: Cloud Computing und IT-Forensik.

Rechtliche Aspekte von Cloud Computing

Wie heutzutage Strom wird in nächster Zukunft Informationstechnologie durch Cloud Computing bildlich gesprochen „aus der Steckdose“ kommen. Cloud Computing liegt die Idee zu Grunde, dass Software

und Daten nicht mehr beim Nutzer verarbeitet oder gespeichert werden. Stattdessen stellt ein Dienstleister Software und Daten dynamisch und nach Bedarf über das Internet bereit und nutzt Rechenkapazität von vielen Rechnern, die teilweise weltweit verteilt sind. Rechenleistung, Speicherkapazität oder Software werden folglich von den Nutzern nur noch bei Bedarf „aus der Wolke“ bezogen und bezahlt.

Cloud Computing ermöglicht eine Zentralisierung von Kapazitäten, die zu Flexibilisierung, Kosteneinsparungen, optimaler Ausnutzung dieser Kapazitäten und dem Schutz der Umwelt führt. Cloud Computing erfährt deshalb gerade einen Wandel

ANZEIGE

MANUFACTURING / ENGINEERING

Procter & Gamble ist eines der erfolgreichsten Markenartikelunternehmen der Welt. In unseren deutschen Werken werden Produkte für den gesamten Weltmarkt gefertigt und zum Teil die Fertigung von Produktionslinien an verschiedenen Standorten Europas betreut.



Praktikum / Abschlussarbeit


Wir bieten:

- 4-6 monatige Projekte mit komplexen technischen Aufgabenstellungen
- Selbstständigkeit und Eigenverantwortung
- Arbeit in jungen dynamischen Teams

Neugierig?

Weitere Infos findest Du unter www.pgcareers.com
Unsere technischen Stellenausschreibungen sind gelistet unter: www.pgcareers.com/technical-ger

Bitte beachte, dass wir nur Online-Bewerbungen annehmen!

Besuche uns auf 



A NEW CHALLENGE EVERY DAY.™
Daily. Globally. Personally. Professionally.

P&G

Das neue IT-Grundrecht

Das „Grundrecht auf Integrität und Vertraulichkeit eigengenutzter informationstechnischer Systeme“ ist durch das BVerfG seit 2008 als Fallgruppe des allgemeinen Persönlichkeitsrechts anerkannt. Es schützt den Einzelnen vor unfreiwilligen Zugriffen auf von ihm genutzte IT-Systeme. Wegen der Allgegenwärtigkeit der Informationstechnik ist der Einzelne darauf angewiesen, sich Systemen anzuvertrauen und bedarf deshalb des staatlichen Schutzes.

vom Trendbegriff zur populären Unternehmensstrategie.

Die diversen Vorteile sind offensichtlich. Das Betriebsrisiko für die Software wird auf Dritte ausgelagert, eine Aktualisierung der Software bei den Kunden ist nicht mehr erforderlich, und die Lizenzgebühren für individuelle Nutzerlizenzen entfallen. Zudem sinkt der Wartungsaufwand für Hard- und Software. Auch die komplette Neuanschaffung ist vielfach nicht mehr nötig. Startups können so ihre Ressourcen und Arbeitszeit in ihr Kerngeschäft investieren. Für bereits etablierte Unternehmen ist die Nutzung von Cloudservices

ANZEIGE



STÄRKE. VIELFALT. SICHERHEIT. UNSERE WERTE FÜR IHRE KARRIERE

In der Elektronik liegt das „versteckte“ Herz jedes Fahrzeuges. AVL-Steuerungssoftware erlaubt Verbrauchsreduktion bei gleichzeitiger Fahrspaß-Steigerung; Lösungen, die millionenfach auf den Straßen unterwegs sind.

Bewerben Sie sich jetzt online unter www.avl.com und gestalten Sie schon heute die Antriebsmethoden von morgen.



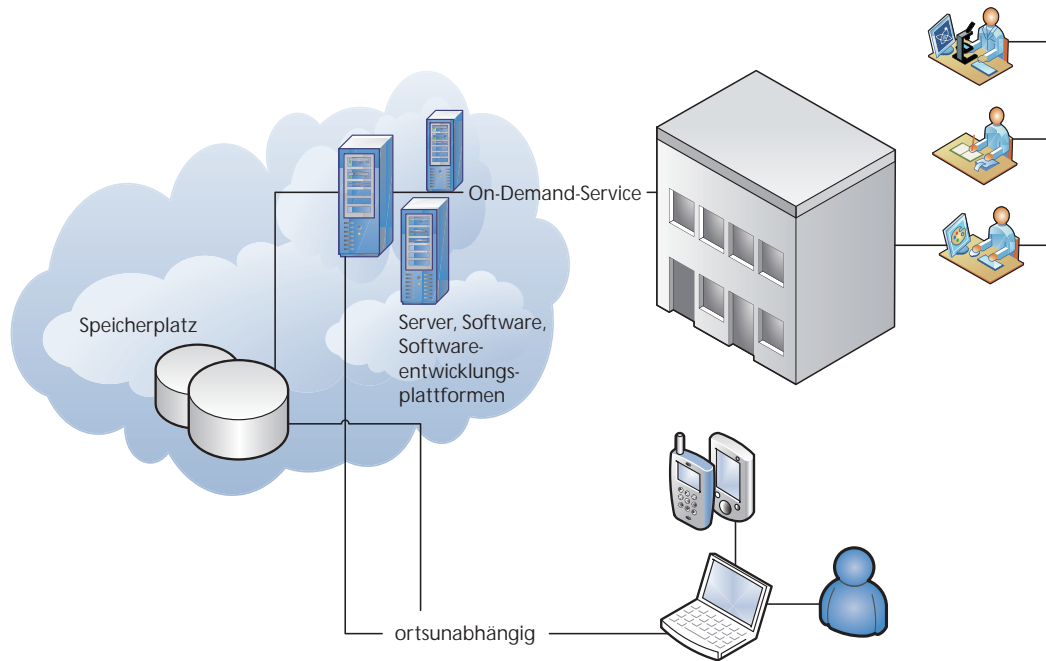


Abbildung 1

Cloud Computing bringt „alles in die Wolke“. Rechenleistung, Speicherplatz, Softwareanwendungen oder sogar Softwareentwicklungsplattformen werden über das Internet als On-demand-Services bereitgestellt. Der Nutzer kann die Dienste ortsunabhängig und flexibel von jedem Gerät aus online nutzen.

projektbezogen oder zum Überbrücken von Lastspitzen denkbar. Diese Bereitstellung von zusätzlichen Optionen und Steuerungsmöglichkeiten ist ein Flexibilitätsaspekt, genauso wie die theoretisch unbegrenzte Skalierbarkeit und Elastizität in einer Cloud oder die Möglichkeit Software-services global und zeitnah an geänderte Anforderungen anzupassen.

Cloud Computing führt jedoch auch zu neuen Gefahren für die in der Wolke vorgehaltenen Daten und zu rechtlichen Problemen. Unabdingbare Voraussetzungen für einen Erfolg am Markt sind demzufolge die Gewährleistung der Sicherheit der Daten und die Klärung der aufgetretenen Rechtsfragen. Dazu zählen insbesondere Fragen des Datenschutzrechts und der damit verbundenen informationellen Selbstbestimmung.

Das anzustrebende Sicherheitsniveau muss dabei mindestens dem bisherigen Stand entsprechen, um die Akzeptanz bei den Nutzern zu gewährleisten. Einige dieser Sicherheitsvoraussetzungen sind rechtlich konkret vorformuliert, überwiegend jedoch abstrakt in Grundrechten und der Rechtsprechung des Bundesverfassungsgerichts als soziale Verhaltens- und Gebotsnormen enthalten. Als konkrete Norm mit Vorgaben zur Datensicherheit sei § 9 BDSG samt Anlage genannt.

Literatur

Niemann, Fabian; Paul, Jörg-Alexander (2009: Bewölkt oder wolkenlos – rechtliche Herausforderungen des Cloud Computings; Kommunikation & Recht)

Pohle, Jan; Ammann, Thorsten (2009: Über den Wolken... – Chancen und Risiken des Cloud Computing; Computer und Recht)

Heinson, Dennis; Yannikos, York; Franke, Frederik; Winter, Christian; Schneider, Markus (2010: Rechtliche Fragen zur Praxis IT-forensischer Analysen in Organisationen; Datenschutz und Datensicherheit)

Heinson, Dennis; Schmidt, Bernd (2010: IT-gestützte Compliance-Systeme und Datenschutzrecht, Computer und Recht, 540)

Auch das weitere Datenschutzrecht, insbesondere die Frage welches Recht anzuwenden ist und inwieweit Daten in Staaten mit einem niedrigeren Datenschutzniveau übermittelt werden dürfen, sind wesentliche Rechtsfragen, die beantwortet werden müssen. Damit einhergehend ist die technische Eigenheit von Public Clouds, dass der tatsächliche Speicherort nicht immer nachvollziehbar ist. Auch die Klärung der Frage, ob und in welchen Fällen eine Auftragsdatenverarbeitung gemäß § 11 BDSG einschlägig ist, muss rechtlich geprüft werden.

Vereinbarungen in Service-Level-Agreements und deren tatsächliche Ausgestaltung sind im Zusammenhang mit Cloud Computing ebenfalls von großer Bedeutung. Gleiches gilt für den Schutz von Betriebsgeheimnissen oder für urheberrechtliche Fragestellungen, insbesondere im Zusammenhang mit Softwarelizenzen.

Cloud Computing ist ein gutes Beispiel für eine aktuelle Fortentwicklung der Informationstechnologie und die damit einhergehenden juristischen Herausforderungen.

Rechtliche Aspekte der IT-Forensik

Weil Informationstechnik mittlerweile fast allgegenwärtig (ubiquitous) ist, bildet ihre Nutzung auch einen immer größeren Teil menschlicher Lebensgestaltung ab. Informationstechnik gewinnt deshalb auch juristisch immer mehr an Bedeutung. Immer öfter ist man auf Daten angewiesen, um Verhalten nachweisen zu können. Elektronische Spuren zu sichern und zu verwerten, ist auch Teil des Forschungsbereichs IT-Forensik bei CASED. Dies ist nicht nur technisch eine Herausforderung, denn immer, wenn es um die Gewinnung und Verwendung von Beweisen geht, muss ein breites Spektrum an rechtlichen Anforderungen berücksichtigt werden.

Fest steht dabei, dass es künftig in vielen Fällen ohne IT-Forensik nicht mehr möglich sein wird,

rechtserhebliches Verhalten nachzuweisen. So gibt es beispielsweise Straftaten, die vollständig innerhalb von IT-Systemen begangen werden können. Bei der Erforschung von Forensikverfahren werden bei CASED deshalb schon frühzeitig Rechtsfragen gestellt. Damit wird sichergestellt, dass etwa Forensiksoftware so gestaltet werden kann, dass sie den strengen rechtlichen Kriterien der Beweissicherheit genügt. Dies ist wiederum nur mit technischem Know-How möglich. Es gilt, technische Unterschiede zu berücksichtigen und eine Bewertung jeweils anhand des eingesetzten Verfahrens vorzunehmen. Denn so vielfältig wie die Informationstechnik den Menschen im Alltag begegnet sind auch die Möglichkeiten, aus ihr die anfallenden Daten zu gewinnen.

Ob aus „der Cloud“, dem Mobiltelefon oder dem Unternehmensnetzwerk: In jedem Anwendungsfeld stellen sich unterschiedliche rechtliche Anforderungen an die Nutzung von Daten zu Beweis Zwecken. Bei der klassischen Datenträgerforensik muss beispielsweise untersucht werden, inwiefern das 2008 erstmals vom deutschen Bundesverfassungsgericht benannte „IT-Grundrecht“ den Nutzer eines Datenträgers vor der Auswertung der Daten schützt. Im Bereich der Live Analyse stellt sich unter anderem die Frage, inwiefern Systemzustände beweissicher nachweisbar sind, wenn Daten im laufenden Betrieb aus einem informationstechnischen System gewonnen wurden. Data Mining oder Maschinelles Lernen sind Techniken, mit denen sich aus großen Datenmengen beispielsweise Verhaltensabweichungen feststellen lassen. Diese Verfahren können auch zu Beweis Zwecken dienen und sind vor allem datenschutzrechtlich problematisch, weil sie bei der Verarbeitung von personenbezogenen Daten (Massenscreenings) bei den Betroffenen schnell ein Gefühl des Überwachtwerdens oder der Generalverdächtigung erzeugen können.

Technische Fragen allein unter dem Gesichtspunkt rechtlicher Anforderungen zu lösen, würde aber den tatsächlichen Anforderungen der IT-Forensik nicht entsprechen. Rechtliche Vorgaben stehen technischen Forderungen nach Effizienz und praktischen Anforderungen hinsichtlich Effektivität gegenüber. Denn trotz aller Bemühungen um Datenvermeidung und Datensparsamkeit sind vielfach Datenberge herangewachsen, bei denen es zur sprichwörtlichen Suche nach der Nadel im Heuhaufen werden kann, Beweise aufzuspüren. Bei CASED sollen deshalb Verfahren entwickelt werden, die zu einem angemessenen Ausgleich der unterschiedlichen Interessen führen – denn auch ein juristisch noch so ausgefeiltes Verfahren hilft nicht, wenn es technisch nicht in der Lage ist, Beweise aufzuspüren.

Informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung ist das Recht des Einzelnen grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Es ist eine Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG und wurde vom Bundesverfassungsgericht im Volkszählungsurteil aus dem Jahr 1983 als Grundrecht anerkannt. Das Urteil hatte maßgeblichen Einfluss auf die Weiterentwicklung des Datenschutzrechts. Das Land Hessen war im Übrigen Vorreiter bei der Kodifizierung des Datenschutzes und verabschiedete bereits am 7. Oktober 1970 das weltweit erste Datenschutzgesetz.

Wie diese beiden Beispiele zeigen, kann rechts-gemäße Technikgestaltung und technikinformierte Rechtsfortbildung entscheidend zur Akzeptabilität und Akzeptanz von Sicherheitslösungen beitragen.



Alexander Roßnagel ist Vizepräsident der Universität Kassel und Direktor des Forschungszentrums für Informationstechnik-Gestaltung (ITeG). Er ist zudem Principal Investigator des LOEWE-Zentrums CASED.



Dennis Heinson ist wissenschaftlicher Mitarbeiter in der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) der Universität Kassel und Stipendiat des Center for Advanced Security Research Darmstadt (CASED).



Mark Bedner ist wissenschaftlicher Mitarbeiter in der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) der Universität Kassel und Stipendiat des Center for Advanced Security Research Darmstadt (CASED).

Sichere Netze

– mit dem Nutzer im Zentrum

Im letzten Jahrzehnt des zwanzigsten und im ersten Jahrzehnt des ein- und zwanzigsten Jahrhunderts hat die weite Verbreitung zweier neuartiger Kommunikationstechnologien die Kommunikation von Menschen drastisch verändert. Der Mobilfunk unterstützt hierbei die persönliche Mobilität von Menschen, und das ubiquitär verfügbare Internet ermöglicht eine Vielzahl von neuartigen Anwendungen, die weit über die klassische Telefonie hinausgehen. Der Schutz der Privatsphäre ist dabei eine wichtige aber bisher nur unzureichend gelöste Herausforderung.

► *Secure Networks – focusing on the user*

In the last decade of the 20th century and in the first decade of the 21st century, the wide distribution of two novel communication technologies changed dramatically the way we communicate. Mobile communications support the user's personal mobility and the new ubiquity of the internet allows a multitude of novel applications, reaching far beyond conventional telephony. Privacy protection in this context is an important but so far inadequately solved challenge.

Matthias Hollick, Thorsten Strufe, Alejandro Buchmann • Mit der Verfügbarkeit kostengünstiger drahtloser Sensoren/Aktoren ist in einem nächsten Schritt zu erwarten, dass Gegenstände des Alltags vernetzt und in der digitalen Welt erreichbar werden. Es findet also eine Vernetzung nicht nur der Menschen und deren „digitaler Repräsentanten“ sondern auch der sie umgebenden „digitalen Helfer“ statt. Eine Vielzahl nützlicher Anwendungen und Szenarien ist denkbar: „Smart Spaces“, „Smart Homes“ und „Smart Cities“. Diese Anwendungen bezeichnet man als smart, weil sie mit der Umwelt interagieren können und sich hierdurch eine Vielzahl von neuen Möglichkeiten eröffnet: Das Sparen von Energie, weil Sensoren eine optimierte Steuerung von Heizung und Licht ermöglichen; die Steigerung der Effizienz in Logistik und Verkehr, weil Sensoren Auskunft geben über Verkehrsflüsse und Staus und eine optimierte Verkehrslenkung erlauben. Darüber hinaus sind die Nutzer selbst und ihre sozialen Gemeinschaften Teil dieser „smarten“ Umgebungen: Sie bilden ihre sozialen Beziehungen aus der realen Welt in Online-Sozialen Netzen ab und ermöglichen damit eine Verknüpfung dieser sozialen Beziehungen mit den erfassten Umweltdaten. Sie erzeugen und konsumieren Informationen – einerseits in klassischen Server-basierten Netzen aber auch direkt unter-

einander in sogenannten Peer-to-Peer Netzen. Sie ergänzen vorhandene Sensoren der Infrastruktur durch ihre mit vielfältigen Sensoren ausgestatteten Mobiltelefone (z. B. Mikrofon, Kamera, Beschleunigungssensoren, GPS) die ihre direkte Umwelt erfassen.

Aus technologischer Sicht bilden Kommunikationsnetze den Nukleus der oben genannten Systeme. Sie zeichnen sich dadurch aus, dass die Anzahl der vernetzten Geräte extrem hoch ist, da auf jeden Einwohner einer „Smart City“ mannigfaltige vernetzte Geräte entfallen. Diese Netze besitzen heterogene Komponenten: Von dedizierten und kabelgebundenen stationären Sensoren bis hin zu hochmobilen Endsystemen, die drahtlos kommunizieren. Eine Vielzahl technologischer Herausforderungen für diese Netze der Zukunft gilt als bisher ungelöst, wie zum Beispiel die Netze hinsichtlich Nutzeranzahl, Ereignismenge, Mobilität, etc. skalierbar zu gestalten. Betrachtet man diese Netze mit dem Menschen im Fokus, so ist der Schutz der Privatsphäre eine wichtige aber bisher nur unzureichend gelöste Herausforderung.

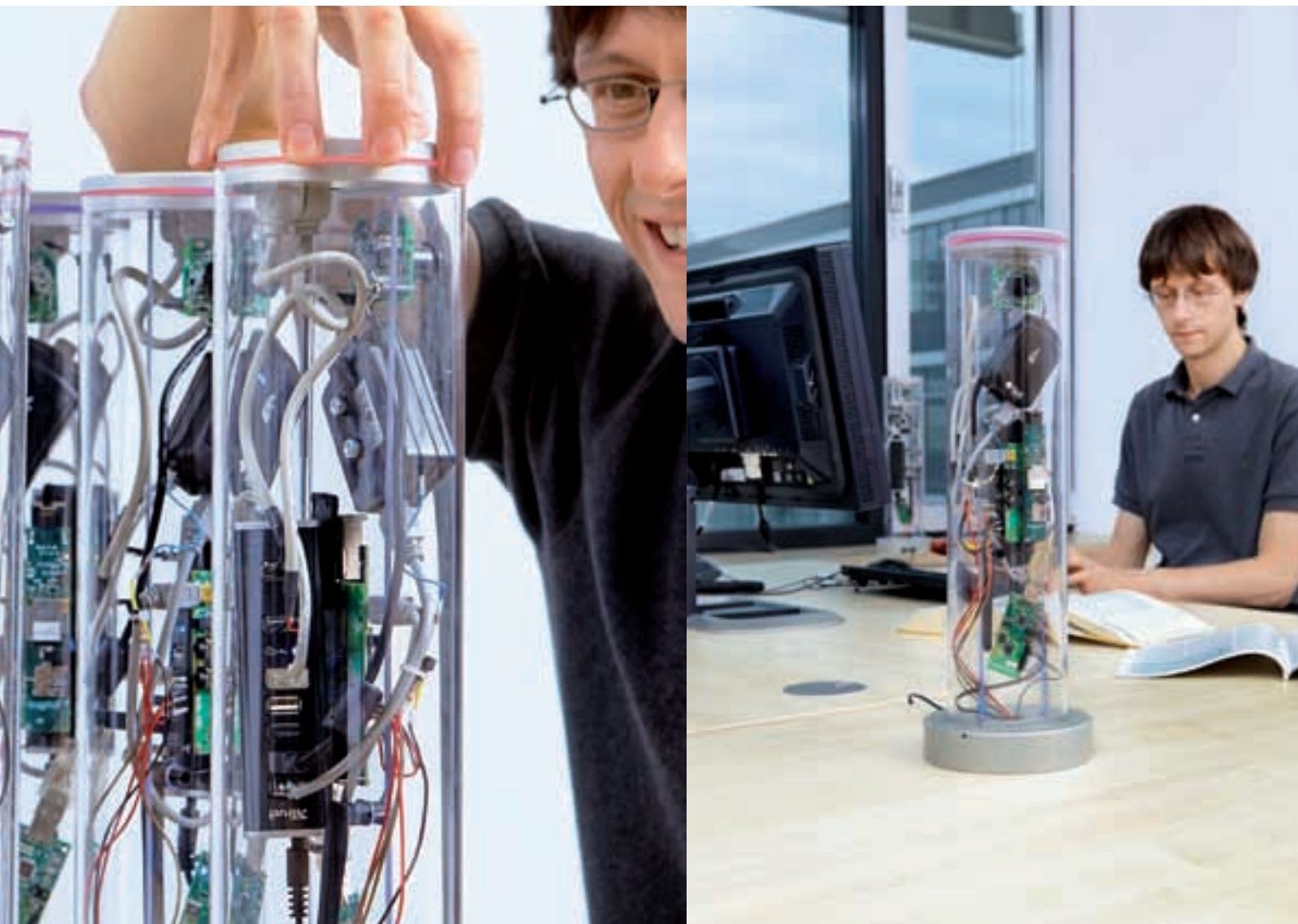
Wieso ist dies der Fall? In „smarten“ Umgebungen wird eine Vielzahl von Daten erhoben, die über einzelne Nutzer Aufschluss geben können. Die Nutzer selbst sind über am Körper getragene Sensoren (zum Beispiel Mobiltelefone) integraler Bestandteil des Monitorings ihrer Umgebung. Soziale Beziehungen zwischen Nutzern sind über Online-Soziale Netze nachvollziehbar. Eine Verknüpfung dieser unterschiedlichen Datenquellen, deren Aggregation oder Anreicherung führt dazu, dass potenziell Bewegungsmuster erstellt werden können und der Schutz der Privatsphäre der Nutzer bedroht ist.

Hier setzen die Arbeiten der Gruppen von Alejandro Buchmann, Matthias Hollick und Thorsten Strufe an, indem sie auf unterschiedlichen Ebenen Beiträge leisten, die den Schutz der Privatsphäre von Nutzern auch für die skizzierten zukünftigen Netze ermöglichen.

Scopes – Ein neues Kommunikationsparadigma für Sensornetze

Das in der Gruppe von Alejandro Buchmann entwickelte Kommunikationsrahmenwerk Scopes wurde speziell auf drahtlose Sensornetze angepasst und ermöglicht, dass die Sichtbarkeit der erfassten Daten eingeschränkt werden kann. Scopes basiert

Matthias Hollick



auf dem Grundprinzip des Publish/Subscribe; hierbei werden von der Datenquelle Ereignisnachrichten erzeugt und kommuniziert, auf Abnehmerseite wird das Interesse an Ereignissen spezifiziert, ein Mediator vermittelt zwischen Quelle und Abnehmer der Ereignisse. Scopes realisiert als ein solcher Mediator dynamische Gruppen innerhalb des Sensornetzes. Diese können auf Basis von Anwendungsklassen („Alle Temperatursensoren“),

geographischen Positionen („Sensoren im Hauptbahnhof“), Systemeigenschaften/-zuständen („Sensoren mit Fehlergenauigkeit kleiner 1%“, „Sensoren mit Restlaufzeit von mindestens 1 Woche“), Schutzleveln („Öffentliche Sensoren“), etc. sowie Kombinationen entsprechender Kriterien („Sensoren zur Messung der Luftqualität in der Rheinstrasse; Restlaufzeit von mindestens 1 Monat“) erstellt und dynamisch verwaltet werden.



Die Einschränkung der Sichtbarkeit von Daten erfordert in Kombination mit Scopes den Einsatz entsprechender angepasster Kryptoverfahren, da klassische identitätsbasierte Verfahren nicht flexibel genug sind. Für den vorgestellten Anwendungsfall bietet sich die attributbasierte Kryptographie an, bei der der Zugriff auf die erhobenen Daten anhand von Attributen der Daten selbst und nach entsprechenden Regeln erfolgt. Gleichzeitig müssen diese Verfahren der attributbasierten Kryptographie für leichtgewichtige Sensorplattformen angepasst werden.

Schutz der Privatsphäre für Sensornetze auf Basis von Mobiltelefonen

Neben dedizierten Sensornetzen wird aktuell die Nutzung von Mobiltelefonen als Sensoren vorangetrieben (sogenannte „partizipative“ Sensornetze). Der Vorteil einer extrem hohen Durchdringung unserer Umwelt mit diesen Sensoren - wo Nutzer sind, sind auch Sensoren - ist gleichzeitig kritisch hinsichtlich des Schutzes der Privatsphäre zu bewerten - eine direkte Zuordnung von Sensor zu Nutzer ist möglich.

In bisherigen Systemen ist der Nutzer zwar in den Prozess der Datenerfassung einbezogen, nicht jedoch in die Abwägungen zum Schutz der Privatsphäre. In der Gruppe von Matthias Hollick werden

daher Lösungen entwickelt, die den Nutzer aktiv in den Prozess der Privatsphäre-bewussten Datenerhebung und -weitergabe einbeziehen. Hierzu wird abweichend von den klassischen Systemen, die eine zentrale Datenbank für erfasste Sensordaten nutzen, ein verteilter Ansatz auf Basis des Peer-to-Peer Paradigmas verfolgt. Dieser baut darauf auf, die erhobenen Daten mit vertrauenswürdigen Nutzern oder vertrauenswürdigen Nutzergruppen zu teilen (diese Beziehungen können bspw. in Online-Sozialen Netzen abgebildet werden). Innerhalb dieser Gruppen sich vertrauender

Thorsten Strufe

Fachgebiet Sichere Mobile Netze

Prof. Dr.-Ing. Matthias Hollick
Tel. 06151/16-70922
E-Mail: matthias.hollick@seemoo.tu-darmstadt.de
www.seemoo.tu-darmstadt.de

Fachgebiet Peer-to-Peer Netzwerke

Prof. Dr.-Ing. Thorsten Strufe
Tel. 06151/16-6774
E-Mail: strufe@cs.tu-darmstadt.de
www.p2p.tu-darmstadt.de

Fachgebiet Datenbanken und Verteilte Systeme

Prof. Alejandro Buchmann, PhD
Tel. 06151/16-6228
E-Mail: buchmann@dvs1.informatik.tu-darmstadt.de
www.dvs.tu-darmstadt.de

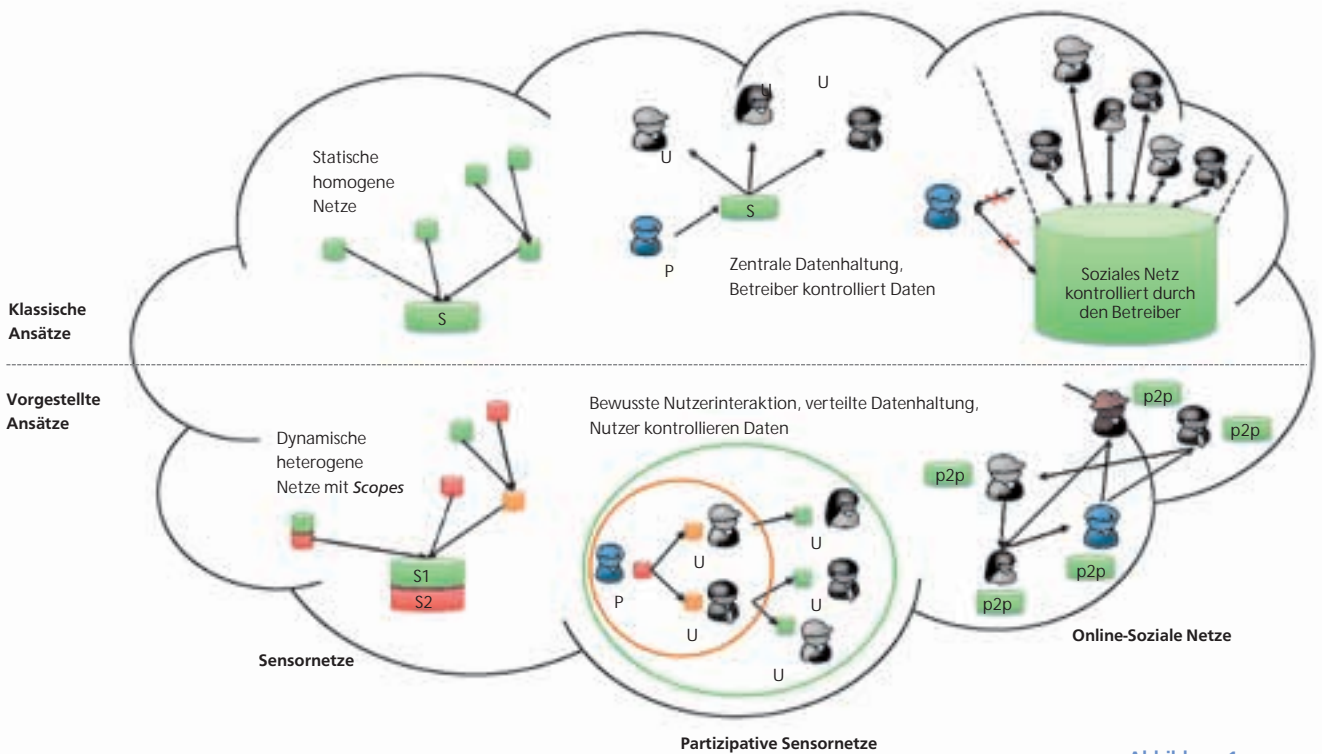


Abbildung 1
Klassische vs. nutzerzentrierte Sicherheit in Netzen

Nutzer erfolgt eine Verschleierung der Identität der Datenquelle, indem sich vertrauende Nutzer die Daten anonymisieren bzw. aggregieren: Mit zunehmender Entfernung von der Datenquelle verringert sich damit die Möglichkeit direkte Rückschlüsse auf die Quelle zu ziehen.

Dem Nutzer fällt bei dem hier verfolgten partizipativen Ansatz eine Schlüsselrolle zu: Die Festlegung der Attribute der erfassten Daten zur Zugriffsbeschränkung sowie die Etablierung von Vertrauensverhältnissen beziehen den Nutzer mit ein. Sensoren des Mobiltelefons werden genutzt, um in direkter Interaktion mit anderen Nutzern Vertrauensbeziehungen bewusst zu etablieren.

Schutz der Privatsphäre in Online-Sozialen Netzen (OSN)

Online-Soziale Netze wie Facebook, LinkedIn, XING, bilden soziale Beziehungen der realen Welt in die virtuelle Welt des Internet ab. Der Schutz der Privatsphäre wird bei diesen Systemen heute von den Betreibern des sozialen Netzes definiert und umgesetzt, häufig zu Lasten des Nutzers, der Privates nur unzureichend schützen kann.

Die Gruppe von Thorsten Strufe erforscht aus diesem Grund die Benutzung, und insbesondere neue Architekturen für Online-Soziale Netze. Dabei steht der bessere Schutz privater Daten der Benutzer im Vordergrund. Auch hier wird das Peer-to-Peer Prinzip verfolgt: Die Daten werden nicht zentral gespeichert und verwaltet sondern verteilt auf den Rechnern der beteiligten Benutzer. Diese können den Zugriff auf ihre Daten feingranular erlauben, oder auf Wunsch – bis hin zu ihrer eigenen vollkommenen Unsichtbarkeit für andere Benutzer – verstecken. Ein allwissender

Zugriff zentraler Instanzen, wie er bisher den kommerziellen Betreibern möglich ist, wird dadurch verhindert.

Fazit

Die vorgenannten Lösungsansätze basieren auf verwandten und sich gegenseitig ergänzenden Grundprinzipien: Die Einschränkung der Sichtbarkeit von Daten; die verteilte Speicherung und Datenhaltung; die Nutzung attributbasierter Zugriffskontrolle und die Einbindung des Nutzers selbst in den Prozess der Attributzuweisung. Gemeinsam erlauben diese Ansätze einen verbesserten und transparenten Schutz der Privatsphäre von Nutzern.



Matthias Hollick ist seit 2009 Professor am Fachbereich Informatik der TU Darmstadt. Er leitet das Fachgebiet „Sichere Mobile Netze“ und ist Principal Investigator des LOEWE-Zentrums CASED.



Thorsten Strufe ist seit 2009 Juniorprofessor am Fachbereich Informatik der TU Darmstadt. Er leitet das Fachgebiet „Peer-to-Peer Netzwerke“ und ist Principal Investigator des LOEWE-Zentrums CASED.



Alejandro Buchmann ist seit 1991 Professor am Fachbereich Informatik der TU Darmstadt. Er leitet das Fachgebiet „Datenbanken und Verteilte Systeme“ und ist Principal Investigator des LOEWE-Zentrums CASED.

Sicher fahren

– Absicherung moderner Fahrzeugsoftware

Moderne Fahrzeuge sind fahrende Computer. Damit eröffnen sich nicht nur neue Chancen, sondern auch neue Fehlerquellen und Angriffsmöglichkeiten. Die TU Darmstadt entwickelt modellbasierte Verfahren zur Überwachung der Fahrzeugsoftware, um diesen neuen Gefahren zu begegnen. Eine strikte Trennung von Überwachungs- und Fahrzeugsoftware erlaubt eine Absicherung von Steuergeräten ohne das Risiko, durch die Aktualisierung der Fahrzeugsoftware selbst neue Fehler einzuführen.

► *Drive safely:* *Securing automotive software*

Modern cars are driving computers. Therewith new risks like software errors and malicious attacks arise. To address these challenges, researchers at TU Darmstadt develop a model-driven approach for monitoring automotive software. By strictly separating monitoring and automotive software the approach succeeds in securing electronic control units without running the risk of introducing new errors into the automotive software itself.

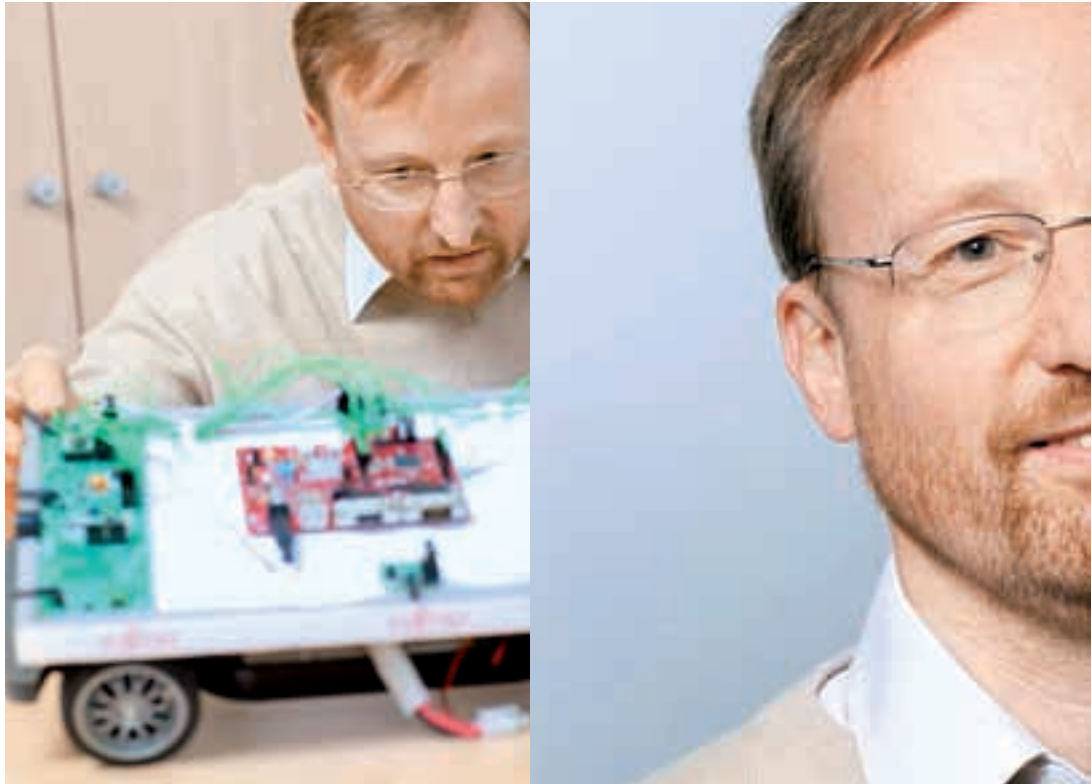
Sven Patzina, Lars Patzina, Eric Bodden, Mira Mezini, Andreas Sewe, Andy Schürr • Getrieben durch technische Innovationen werden eingebettete Systeme zunehmend stärker untereinander vernetzt und bieten Kommunikationsschnittstellen an. War früher zur Manipulation physischer Zugriff auf die Steuergeräte nötig, ist dies bei aktuellen Systemen nicht mehr erforderlich. Heutzutage können sie nicht als von der Außenwelt abgeschlossene Einheiten angesehen werden, obwohl sie oftmals als solche entwickelt wurden. Bei ihrer Spezifikation wurde häufig wenig Aufmerksamkeit auf Sicherheitsmechanismen wie Verschlüsselung und sicheres Komponenten-Design zur Abwehr von Angriffen von außen gelegt. Die Forschung hat jedoch gezeigt, dass moderne Netzwerke in Autos solche Sicherheitsmechanismen benötigen [1]. Zur nachträglichen Absicherung dieser Systeme ist es daher erforderlich, eine abgesicherte Kommunikation im Auto und eine sichere Architektur zur Verbesserung der Privacy und der Security zu entwickeln [3]. Selbst bei der Neuentwicklung eingebetteter Systeme, bei der alle empfohlenen Verfahren durchgeführt werden, ist es meist nicht möglich, alle Sicherheitslücken zu eliminieren und jeden möglichen Angriff vorherzusehen. Betrachtet man große heterogene Systeme oder Dienste und will



Mira Mezini



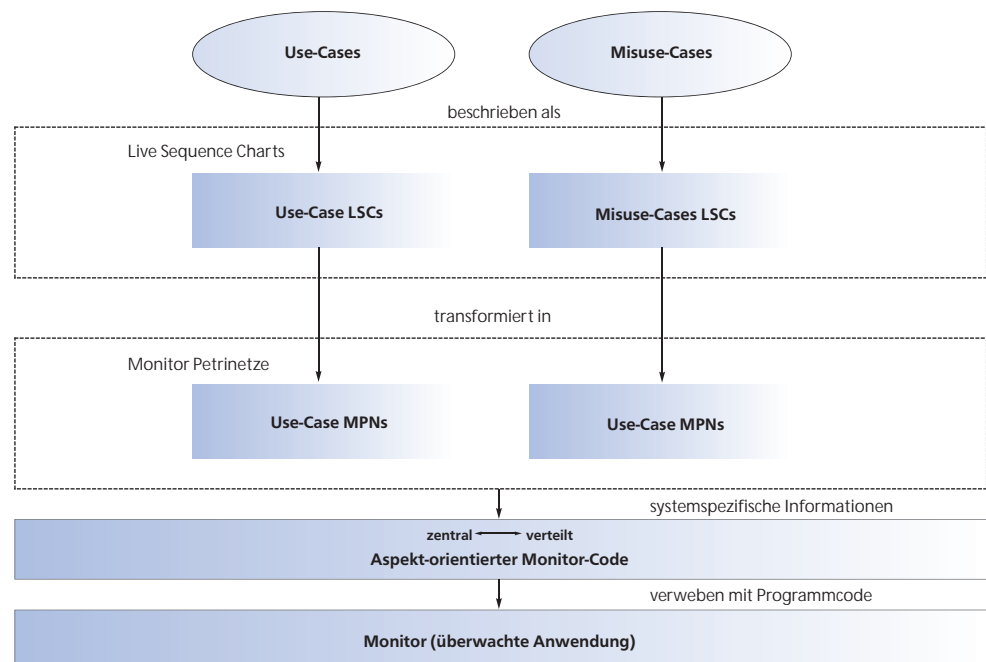
Andy Schürr



diese nachträglich absichern, ist dies meistens ökonomisch oder technisch nicht zu realisieren. Resultierend daraus kann bei keinem System davon ausgegangen werden, dass es sicher ist – sei es durch unbekannte Schwachstellen oder durch die Verwendung von Legacy-Komponenten, die nicht mehr angepasst werden können.

Wenn die bei der Spezifikation und Implementierung umgesetzten Sicherheitsmechanismen überwunden wurden, steht einem Angriff nichts mehr im Wege. Der Hersteller müsste eine Rückrufaktion starten und die Schwachstellen beheben, um seine Kunden vor der Bedrohung zu schützen. Eine Auslieferung von neuer Software, wie es vom PC über

Abbildung 1 Modellbasierter Security-Monitor-Generierungsprozess. Im Rahmen der CASED-Forschungen an der TU Darmstadt wird ein modellbasierter Entwicklungsprozess entworfen, der es in Zukunft der Industrie ermöglichen wird, Monitore vollautomatisch aus grafischen Spezifikationen zu generieren. Ohne diesen Prozess ist die Entwicklung des Monitors ähnlich komplex wie Änderungen am System selbst. Der modellbasierte Ansatz hilft Fehler zu vermeiden.



einen Funkkanal bzw. das Internet bekannt ist, stellt im Bereich der eingebetteten Systeme ein hohes Sicherheitsrisiko dar, da ein fehlerhaftes Update schwerwiegende Konsequenzen haben kann.

Im Automobilbereich ist ein Update der Multi-mediakomponenten noch vorstellbar, der Eingriff in sicherheitskritische Steuergeräte jedoch nicht zu vertreten.

Um kostenintensive Maßnahmen bis zum nächsten regulären Service-Termin in der Werkstatt hinauszuzögern, ist eine weitere Instanz nötig: Ein Monitor, der in Software oder Hardware umgesetzt sein kann, überwacht die Kommunikation verschiedener Komponenten untereinander oder die Komponenten selbst. Dabei kann er abweichendes oder auf Angriffe schließendes Verhalten erkennen und gegebenenfalls Gegenmaßnahmen einleiten [2]. Diese Monitore könnten im Fall einer neuen nicht abgedeckten Sicherheitslücke um neue Signaturen erweitert werden und dadurch die Lücke erkennen und absichern, ohne dass eine Anpassung der kritischen Systeme notwendig wäre.

Detaillierte Beschreibung der Abläufe als Life Sequence Charts

Was passiert nun im Detail? Die Sequenzen, die die (Mis-)Use-Cases beschreiben, werden als Life Sequence Charts (LSCs) modelliert. Diese Charts bie-

ten die Möglichkeit optionale („cold“) und erforderliche („hot“) Nachrichten zu spezifizieren. Abbildung 2b beschreibt ein Muster für das oben als Misuse-Case definierte Fehlverhalten des Tempomaten. In diesem Szenario müssen vier Instanzen - der Fahrer, der Tempomat, das Fahrzeug und der Sensor für die Abstandsbestimmung - und deren Kommunikation untereinander betrachtet werden. Während der Fahrt kann der Fahrer die Geschwindigkeit des Tempomats beliebig oft anpassen (setzeGeschwindigkeit()). Entschidet sich der Fahrer den Tempomat zu aktivieren (starteRegelung()), sendet dieser die vorher gesetzte Sollgeschwindigkeit an das Fahrzeug. Hat der Sensor

ANZEIGE

Literatur

[1]C. Groll, A. ; Ruland. Secure and authentic communication on existing in-vehicle networks. In Intelligent Vehicles Symposium, 2009 IEEE, pages 1093-1097, Inst. for Data Commun. Syst., Univ. of Siegen, Siegen, Germany, July 2009.

[2]Michael Müter, Tobias Hoppe, and Jana Dittmann. Decision model for automotive intrusion detection systems. In Automotive - Safety & Security 2010, pages 103-116. Shaker Verlag, 2010.

[3]P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Zhendong Ma, F. Kargl, A. Kung, and J. P. Hubaux. Secure vehicular communication systems: design and architecture. IEEE Communications Magazine, 46(11): 100-109, November 2008.

[4]Lars Patzina, Sven Patzina, Thorsten Piper, and Adny Schürr. Monitor Petri Nets for Security Monitoring. In ICPS of International workshop on S&D4RCEs 2010. ACM.

INNOVATIVE
TECHNOLOGIE
WELTWEIT



NEUBERGER

MEMBRANPUMPEN- TECHNOLOGIE VOM FEINSTEN...

■ Ob für Gase, Dämpfe oder Flüssigkeiten – KNF Neuberger bietet ein breites Angebot an Pumpen und Systemen.

■ Für unverfälschtes Fördern, Dosieren, Komprimieren und Evakuieren.

■ Als OEM- oder tragbare Ausführungen.

■ Mit einem variablen Produktprofil für kundenspezifische Lösungen.

... für anspruchsvolle Anwendungen – z.B. in den Bereichen:

- Medizintechnik
- Analysetechnik
- Verfahrenstechnik
- Lebensmitteltechnik
- Reptechnik
- Energietechnik
- Forschung



www.knf.de

KNF Neuberger GmbH ■ Alter Weg 3 ■ D 79112 Freiburg
Tel. 07664/5909-0 ■ Fax 07664/5909-99 ■ E-Mail info@knf.de

eine Abstandsunterschreitung festgestellt, sendet er die Nachricht „abstandUnterschritten()“ an das Fahrzeug. Geschieht dies, wird das Muster erkannt und der Zustand „FALSE“ erreicht. Der mit der Abhängigkeit „mitigate“ dem Misuse-Case zugeordnete Use-Case „Beschleunigung unterdrücken“ wird nun ausgeführt und verhindert die Beschleunigung auf die Sollgeschwindigkeit.

Transformation zu Monitor-Petrinetzen

Obwohl das Beispiel absichtlich einfach gehalten wurde, können in der Praxis sehr leicht komplexe LSCs entstehen. Dadurch ist die Extraktion aller möglichen Abläufe, die durch das LSC beschrieben sind, sehr aufwändig. Um die Generierung von Monitoren zu vereinfachen, werden die LSCs in sogenannte Petrinetze mit einer speziellen Ausführungsemantik (Monitor-Petrinetze) transformiert [4]. Das Petrinetz für das LSC des Misuse-Cases ist in Abbildung 2c dargestellt. Für jede Instanz im LSC, wie Fahrer, Tempomat, Fahrzeug und Sensor, gibt es einen Startplatz, der eine Marke enthält.

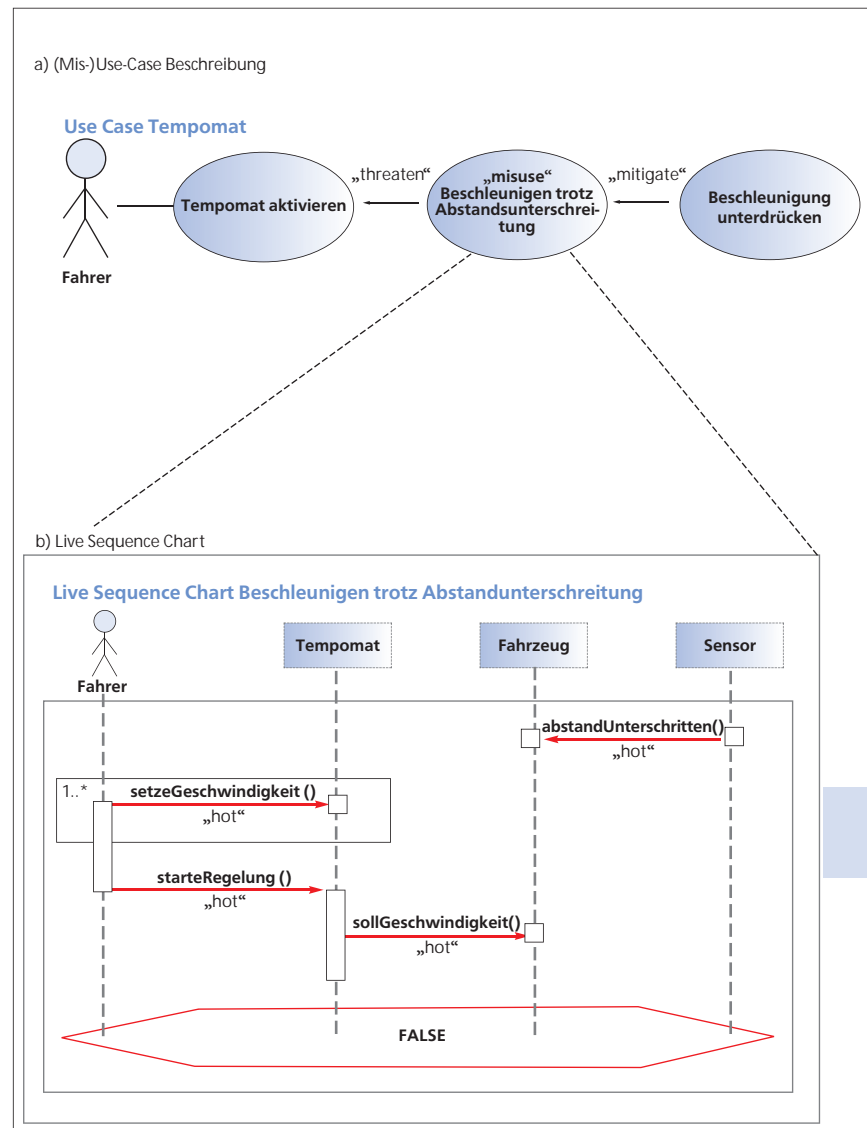
Jede Nachricht des LSCs wird durch Transitionen, die den Übergang der Marken zwischen den Plätzen regeln, repräsentiert. Diese werden durch Ereignisse wie das Senden (s) und das Empfangen (r) einer Nachricht ausgelöst. Sind alle Plätze, die einlaufende Kanten in die Transition haben (Vorplätze), mit Marken belegt und das Ereignis der Transition tritt ein, schaltet diese. Alle Marken auf Plätzen vor der Transition werden konsumiert und auf den nachfolgenden Plätzen neu erzeugt. Auf diese Art stellt das Petrinetz alle möglichen Abläufe des LSC in einer einfach zu interpretierenden Weise dar. Aus diesen Petrinetzen wird dann mit Hilfe von system-spezifischen Informationen die Implementierung des Monitors generiert.

Verweben der Monitore

Die resultierenden Monitore müssen dann in einem letzten Schritt mit dem konkreten Programmcode verbunden (verwoben) werden. Dazu haben sich in den vergangenen Jahren Technologien der aspektorientierten Programmierung sehr bewährt. Aspektorientierte Programme erlauben es, die abstrakten Ereignisse des Monitors auf konkrete Programmereignisse abzubilden.

Viele etablierte Verfahren zur aspektorientierten Programmierung verweben die Monitore schon früh mit der Anwendung. Dies hat allerdings zur Folge, dass es zur Ausführungszeit nur schwer möglich ist, zwischen Überwachungslogik und Applikation zu unterscheiden. Die Aktualisierung eines Monitors zur Laufzeit der Applikation ist somit äußerst kompliziert, da sich die vorherige Version nicht rückstandsfrei entfernen lässt.

An der TU Darmstadt wurden daher Techniken entwickelt, um der Ausführungsumgebung zur Lauf-



zeit alle relevanten Informationen über die Überwachungslogik zur Verfügung zu stellen. Dadurch wird die Ausführungsumgebung in die Lage versetzt, Monitore zur Applikation hinzuzufügen oder zu entfernen, ohne dass die Applikation neu gestartet werden muss.

Fachgebiet Softwaretechnik

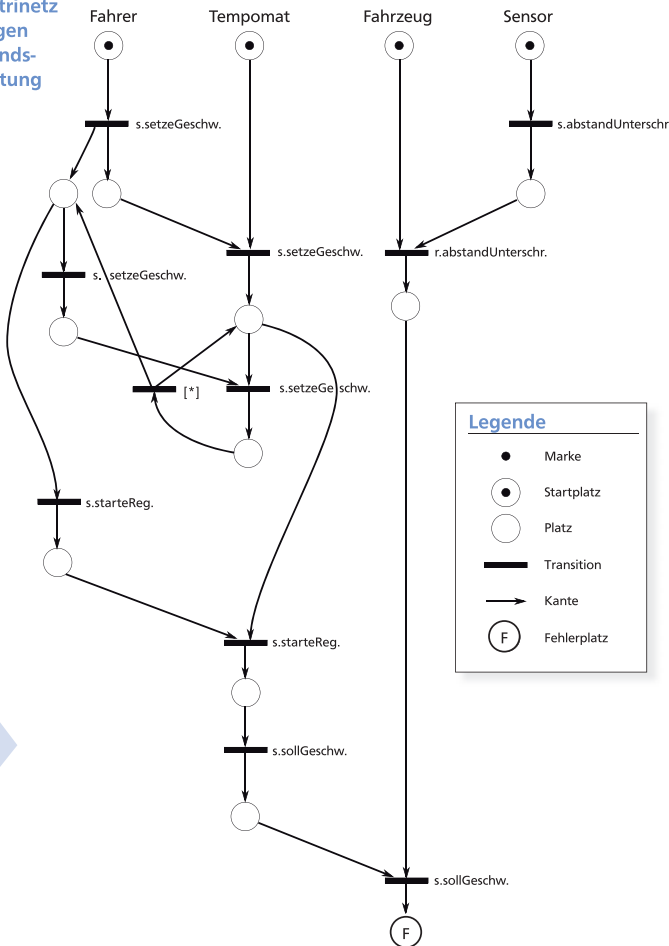
Dr.-Inform. Eric Bodden
Tel. 06151/16-5478
E-Mail: eric.bodden@cased.de
www.stg.tu-darmstadt.de/staff/eric_bodden

Prof. Dr.-Ing. Mira Mezini
Tel. 06151/16-5311
E-Mail: mira.mezini@cased.de
www.stg.tu-darmstadt.de/staff/mira_mezini/

Dipl.-Math. Andreas Sewe
Tel. 06151/16-3608
E-Mail: andreas.sewe@cased.de
www.stg.tu-darmstadt.de/staff/andreas_sewe/

c) Monitor-Petrinetz

Monitor-Petrinetz
Beschleunigen
trotz Abstands-
unterschreitung



Übersetzung

Zusammenfassend lässt sich sagen, dass IT-Sicherheit auch im Automotive-Bereich schon heute von herausragender Bedeutung ist. Verfahren wie das vorgestellte werden daher bald unerlässlich sein, um die Sicherheit der Verkehrsteilnehmer zu gewährleisten.

Fachgebiet Echtzeitsysteme

Dipl.-Ing. Lars Patzina
Tel. 06151/16-3676
E-Mail: lars.patzina@cased.de
www.cased.de/ueber/mitarbeiter.html

Dipl.-Ing. Sven Patzina
Tel. 06151/16-3676
E-Mail: sven.patzina@es.tu-darmstadt.de
www.es.tu-darmstadt.de/mitarbeiter/sven-patzina/

Prof. Dr. rer. nat. Andy Schürr
Tel. 06151/16-6940
E-Mail: andy.schuerr@es.tu-darmstadt.de
www.es.tu-darmstadt.de/mitarbeiter/andy-schuerr/

Abbildung 2

Monitor-Entwicklungsprozess am Beispiel des Tempomaten. Als adäquates Mittel zur Erfassung von funktionalen Anforderungen hat sich die Modellierung mit Use-Cases herausgestellt. Zur Darstellung nicht-funktionaler Anforderungen werden Misuse-Cases verwendet, die das Fehlverhalten des Systems beschreiben. Abbildung 2a zeigt unser Beispielszenario. Ein Auto verfügt über einen Tempomaten. Wenn der Fahrer den Tempomaten betätigt, beschleunigt das Fahrzeug auf eine vorgegebene Geschwindigkeit. Ein Angreifer könnte diese Funktionalität nutzen, um einen Auffahrunfall zu provozieren. Der Fahrzeughersteller macht sich daher die im Fahrzeug vorhandene Entfernungskontrolle zunutze und definiert den Misuse-Case „Beschleunigen trotz Abstandsunterschreitung“. Dieser soll durch einen Monitor erkannt und durch den Use-Case „Beschleunigung unterdrücken“ unterbunden werden.



Eric Boddien ist Post-Doc am Lehrstuhl für Softwaretechnik der TU Darmstadt. Dort befasst er sich mit statischer Programmanalyse und der Optimierung von Laufzeitmonitoren.



Lars Patzina ist seit 2007 Promotionsstipendiant bei CASED und forscht an einem durchgängigen Entwicklungsprozess zur automatischen Generierung von Security-Monitoren.



Sven Patzina ist seit 2007 wissenschaftlicher Mitarbeiter am Fachgebiet Echtzeitsysteme der TU Darmstadt. Seine Forschung umfasst die modellbasierte Spezifikation von Security-Monitoren.



Andreas Sewe studierte Mathematik an der TU Darmstadt und beschäftigt sich nach seinem Abschluss im Rahmen seiner Promotion am Fachgebiet Softwaretechnik mit virtuellen Maschinen.



Mira Mezini ist seit 2002 Professorin am Lehrstuhl für Softwaretechnik der TU Darmstadt. Ihre Forschungsinteressen sind u. a. modulare Programmierparadigmen, statische und dynamische Programmanalysen sowie intelligente Softwareentwicklungsumgebungen.



Andy Schürr ist seit 2002 Professor am Institut für Datentechnik an der TU Darmstadt. Seine Forschungsthemen sind u. a. modellbasierte Softwareentwicklung von eingebetteten Systemen sowie Modelltransformationen- und Spezifikationsprachen.

Sicherheitsgarantien

zuverlässig nachweisen

Die Sicherheit von Softwaresystemen zuverlässig zu garantieren stellt eine große Herausforderung dar, die sowohl theoretische als auch praktische Aspekte beinhaltet. Im Fachgebiet Modellierung und Analyse von Informationssystemen (MAIS) werden mathematisch fundierte Methoden und Werkzeuge entwickelt, die eine präzise Modellierung und einen verlässlichen Nachweis von Sicherheitsanforderungen ermöglichen.

► *Reliable assurance of security guarantees*

Guaranteeing the security of critical software systems is a major challenge that comprises theoretical as well as practical aspects. The chair for Modeling and Analysis of Information Systems (MAIS) develops methods and tools with solid mathematical foundations to support the precise modeling of security requirements and the reliable assurance of security guarantees.

Heiko Mantel • Die korrekte Funktionsweise von Software ist in vielen Anwendungsbereichen unabdingbar. Fehler in der Steuerung von Fahrzeugen können Leib und Leben von Passagieren bedrohen, fehlerhafte Dienste die Reputation ihrer Anbieter gefährden und Verluste von Daten enorme wirtschaftliche Schäden verursachen. Um derartige Zwischenfälle zu vermeiden, sollten kritische Aspekte von Softwaresystemen möglichst zuverlässig garantiert werden. Hierbei kann man sich der Präzision mathematisch fundierter Konzepte und Methoden bedienen.

In den letzten Jahrzehnten wurden in der Entwicklung solcher formaler Methoden in der Informatik signifikante Fortschritte erreicht. Inzwischen gibt es eine Vielzahl formaler Notationen und Kalküle, mit denen das Verhalten von Systemen elegant modelliert und kritische Systemeigenschaften präzise beschrieben und nachgewiesen werden können. Komplexe Verifikationsaufgaben lassen sich mit Hilfe von strukturierten Spezifikationen und Kompositionalitätsresultaten in weniger komplexe Probleme zerlegen, die dann mit modernen Verifikationswerkzeugen weitgehend automatisch bewiesen werden können. Durch diese Fortschritte ist sogar die Verifikation komplexer Softwaresysteme praktisch möglich geworden.

Beim Nachweis von Sicherheitsanforderungen, die die Vertraulichkeit von Informationen oder die Integrität von Daten betreffen, ergeben sich besondere Herausforderungen. Diese betreffen nicht



Heiko Mantel



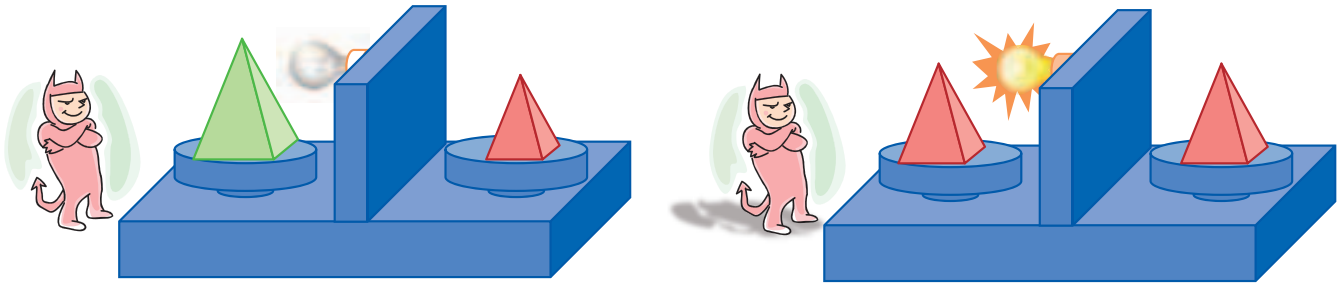


Abbildung 1
Verhinderung unerlaubter Informationsflüsse durch Noninterference

nur den formalen Nachweis kritischer Anforderungen, sondern oft auch die vorausgehende formale Modellierung.

Betrachtet man konzeptionell einfache Sicherheitsmechanismen wie Zugangs- oder Zugriffskontrollen, so ist das Vorgehen noch mit der klassischen Verifikation der Korrektheit von Algorithmen vergleichbar. Aber schon bei der Verifikation kryptographischer Protokolle treten Besonderheiten auf. Neben den durch ein Protokoll vorgegebenen Aktionen müssen auch alle erdenklichen Aktionen potenzieller Angreifer modelliert und bei der Verifikation berücksichtigt werden. Betrachtet man noch komplexere Softwaresysteme, so kann bereits die angemessene Formulierung von Sicherheitsanforderungen zu einer nicht trivialen Herausforderung werden.

Kritische Eigenschaften sollten sowohl präzise als auch möglichst verständlich beschrieben werden, um überzeugende Sicherheitsgarantien zu erhalten. Dass die Erreichung dieser beiden Ziele nicht einfach ist, wird offensichtlich, wenn man typische Anfragen der Sicherheitsinfrastruktur betrachtet. Selbst wenn die korrekte Funktionsweise einer Zugriffskontrolle zweifelsfrei erwiesen ist, sind Aussagen wie „Das Programm Finanzverwaltung versucht, auf das Internet zuzugreifen (Ziel-IP: 141.90.10.11).“ in ihren Folgen kaum überschaubar. Beispielsweise bleibt unklar, in welcher Weise das Internet durch das Programm verwendet werden soll, welche Informationen an andere weitergegeben werden und inwieweit erhaltene Nachrichten Veränderungen der eigenen Daten bewirken. Derartige Formulierungen von Sicherheitsaspekten bieten daher keine adäquate Basis, um Anfragen wie „Wollen Sie diesen Zugriff erlauben?“ fundiert zu beantworten.

Ein Nutzer ist vor allem daran interessiert, was nach einer Zustimmung mit seinen Daten und Res-

Noninterference

Bei der Geheimhaltung von Daten reicht es nicht aus, die direkte Weitergabe dieser Daten zu verhindern. Es muss auch ausgeschlossen werden, dass Angreifer mit Hilfe von erhaltenen Informationen Rückschlüsse über Geheimnisse ziehen können (vgl. Abb. 1). Die Noninterference-Eigenschaft verhindert solche unerlaubten Informationsflüsse, indem sie verlangt, dass Ausgaben (links der Trennwand) an nicht vertrauenswürdige Nutzer von Geheimnissen (rechts der Trennwand) unabhängig sein müssen.

ourcen passieren wird. Mit den Termini und der Funktionsweise technischer Sicherheitsmechanismen sollte er möglichst wenig behelligt werden. Daher wären Formulierungen, wie „Das Programm Finanzverwaltung möchte private Daten aus dem Verzeichnis STEUERERKLÄRUNG-2010 versenden. Diese Daten werden ausschließlich an die Ziel-IP: 141.90.10.11 (Finanzamt) übertragen. Weitere private Daten werden nicht übertragen. Wollen Sie diese Übertragung erlauben?“ deutlich geeigneter, um eine fundierte Entscheidung zu treffen. Weiterhin wäre es wünschenswert, wenn Antworten auf solche Detailentscheidungen in möglichst vielen Fällen aus zuvor angegebenen Sicherheitsbedürfnissen automatisch abgeleitet werden könnten. Zur Erreichung beider Ziele ist es notwendig, die Informationsflüsse und Ressourcennutzungen während einer Programmausführung präzise zu charakterisieren. Allerdings ist die formale Modellierung dieser Aspekte oft nicht einfach.

Um überzeugende Sicherheitsgarantien zu erhalten, ist es außerdem notwendig, dass diese zuverlässig nachgewiesen werden. Aktuelle Forschungsarbeiten in den Bereichen Informationsflusskontrolle und Nutzungskontrolle gehen die Problematik der adäquaten Modellierung und der Verifikation von Sicherheitsaspekten an.

Bereits Anfang der 80er Jahre wurde die Noninterference-Eigenschaft als formal definiertes Kriterium für die Sicherheit des Informationsflusses in



einem System vorgeschlagen. Diese Eigenschaft hat sich inzwischen als Basis für präzise, formale Modellierungen von Informationsflusssicherheit etabliert.

Noninterference schließt nicht nur die unmittelbare Weitergabe vertraulicher Daten an nicht vertrauenswürdige Nutzer aus, sondern auch die Möglichkeit, dass Angreifer aus erhaltenen Daten vertrauliche Informationen errechnen können. Die zu Grunde liegende Idee ist, dass Ausgaben, die völlig unabhängig von Geheimnissen sind, einem Angreifer nicht helfen können, Informationen über diese Geheimnisse zu gewinnen. Diese Forderung führt zu sehr überzeugenden Sicherheitsgarantien, ist allerdings auch sehr restriktiv.

Manchmal ist es wünschenswert oder sogar unabdingbar, dass einige Informationen über vertrauliche Daten bekannt werden. Beispielsweise sollten Filme oder Lieder in einem Online-Shop für Nutzer vor einer Bestellung bzw. Bezahlung nicht zugänglich sein, danach aber schon.

Eine solche Deklassifikation von Informationen, die ursprünglich als vertraulich eingestuft waren, ist auch bei einer Authentifizierung unumgänglich. Aus der Reaktion auf eine Passworteingabe wird offensichtlich, ob das richtige Passwort eingegeben wurde, also ein Rückschluss auf das im System gespeicherte Passwort möglich wird. Deklassifikation muss auch zugelassen werden, wenn die Übertragung von geheimen Daten über ein offenes

Netzwerk nach einer kryptographischen Verschlüsselung erlaubt werden soll.

Um die kontrollierte Preisgabe von Geheimnissen in solchen Fällen zuzulassen, muss die ursprüngliche Definition von Noninterference abgeschwächt werden. Die Entwicklung von Varianten der Noninterference-Eigenschaft, die kontrollierte Deklassifikation unterstützen, spielt für die praktische Verwendung eine zentrale Rolle, ist aber immer noch ein aktuelles Forschungsproblem. Weitere Varianten der Noninterference-Eigenschaft werden erforscht, um gängige Programmierparadigmen besser zu unterstützen. Vor allem die angemessene Behandlung nebenläufiger und verteilter Programmausführung stellt hierbei eine Herausforderung dar.

In diesen Bereichen konnte das Fachgebiet MAIS in den letzten Jahren einige vielversprechende Fortschritte erzielen. Beispielsweise wurden Varianten der Noninterference-Eigenschaft entwickelt, die eine flexible Kontrolle der Deklassifikation ermöglichen bzw. nebenläufige und verteilte Programmausführungen unterstützen. Neben der Entwicklung adäquater Modellierungen von Sicher-

Fachgebiet Modellierung und Analyse von Informationssystemen (MAIS)

Prof. Dr.-Ing. Heiko Mantel

Tel. 06151/16-6651

E-Mail: mantel@mais.informatik.tu-darmstadt.de

www.mais.informatik.tu-darmstadt.de



Abbildung 3
Durchsetzung
von Sicherheits-
anforderungen
durch Kapselungen
(links: gewöhnlicher
Dienst, rechts:
gekapselter Dienst)



heitsanforderungen ist auch die Entwicklung von Techniken und Werkzeugen, die die Verifikation von Informationsflusssicherheit erleichtern, ein aktueller Forschungsgegenstand. Die Erforschung von Ansätzen zur Informationsflusskontrolle wird in den nächsten Jahren durch das von der DFG geförderte Schwerpunktprogramm „Reliably Secure Software Systems“ viele neue Impulse erhalten. Eine weitere konzeptionelle Herausforderung beim Nachweis von Sicherheitsgarantien entsteht durch die Verwendung von Abstraktionen, die für eine Verifikation komplexer Systeme unabdingbar ist (vgl. Abbildung 2). In der Informatik übliche und weit erprobte Abstraktionstechniken sind für Sicherheitsaspekte problematisch. Selbst wenn man bewiesen hat, dass alle Informationsflüsse innerhalb eines Anwendungsprogramms den Sicherheitsbedürfnissen entsprechen, können vertrauliche Daten durch Informationslecks in tiefer liegenden Systemschichten bekannt werden. Ein eng verwandtes Problem tritt bei der Verwendung von abstrakten Spezifikationen in einer schrittweisen Softwareentwicklung auf. Die Abstraktion von technischen Details ist für Spezifikationen hilfreich, kann aber sowohl Möglichkeiten zur Kommunikation zwischen Angreifern (sogenannte verdeckte Kanäle) als auch zur unbeabsichtigten Preisgabe von Geheimnissen (sogenannte Seitenkanäle) bei einer Sicherheitsanalyse verdecken. Um diese Problematiken beherrschbar zu machen, werden im Fachgebiet MAIS im Rahmen der durch die DFG geförderten Nachwuchsgruppe „Formal Methods for Security Engineering“ Techniken zur schrittweisen Entwicklung sicherheitskritischer Software und zur

Analyse verdeckter Kanäle entwickelt. Techniken und Werkzeuge zur Entdeckung und Entfernung von Seitenkanälen in kryptographischen Algorithmen, die durch Unterschiede in der Laufzeit entstehen, werden im Rahmen von CASED entwickelt. Erhält ein Softwaresystem auch während der Ausführung vertrauliche Eingaben, so ist es oft sinnvoll, die statische Sicherheitsanalyse des Programmcodes um eine dynamische Analyse zu ergänzen. Das Konzept der Sicherheitsautomaten erlaubt eine flexible Beschreibung von Komponenten zur Überwachung von Sicherheitseigenschaften zur Laufzeit eines Programms. Sicherheitsbedürfnisse werden als Richtlinien formuliert, deren Einhaltung der Sicherheitsautomat während der Programmausführung überwacht. Sollte die Verletzung einer Sicherheitsrichtlinie bevorstehen, so wird die Programmausführung gestoppt. Werden alle Sicherheitsbedürfnisse durch Sicherheitsrichtlinien erfasst, so kann auf eine statische Sicherheitsanalyse des Programms verzichtet werden. Der Sicherheitsautomat realisiert dann eine Kapselung, die die Umgebung vor Fehlverhalten des Programms und das Programm vor Fehlverhalten nach fehlerhaften Eingaben der Umgebung bewahrt. Um die Anwendungsmöglichkeiten solcher Kapselungen zu erweitern, wurden verschiedene Varianten der Ende der 90er Jahre vorgeschlagenen Definition von Sicherheitsautomaten entwickelt. Editierautomaten erlauben zum Beispiel neben dem Anhalten des Programms im Fehlerfall auch das Unterdrücken oder Abändern einzelner Aktionen des Programms. Das im Rahmen von CASED entwickelte Konzept der Dienstautomaten zielt auf die dynamische Überwachung von Diensten in verteilten Systemen. Dezentrale Monitor-komponenten kommunizieren und kooperieren miteinander. Hierdurch wird eine flexible und zuverlässige Kontrolle der Nutzung sicherheitskritischer Daten und Ressourcen unterstützt, die der modularen und verteilten Architektur moderner dienstorientierter Systeme Rechnung trägt.



Heiko Mantel ist seit 2007 Professor an der TU Darmstadt. Er leitet das Fachgebiet Modellierung und Analyse von Informationssystemen (MAIS) im Fachbereich Informatik. Er koordiniert das DFG-Schwerpunktprogramm „Reliably Secure Software Systems“ und ist zudem Principal Investigator des LOEWE-Zentrums CASED.

IKT-Unterstützung

erhöht Sicherheit in Stress-Situationen

Bei einer Großschadenslage, wie z. B. einem Chemieunfall oder einem Großbrand, werden extreme Anforderungen an die Belastbarkeit der menschlichen Einsatzkräfte, an die Schnittstelle zwischen Mensch und Technik sowie an die Technik selbst gestellt. Notwendige Absprachen der Rettungskräfte sind aufgrund der angespannten und oftmals von Stress geprägten Situation besonders fehleranfällig, kosten permanent Zeit und lenken viel Aufmerksamkeit von der eigentlichen Aufgabe ab. Informations- und Kommunikationstechnik (IKT) kann die Öffentliche Sicherheit mit verschiedenen Maßnahmen unterstützen, damit angemessen auf eine Großschadenslage reagiert werden kann. Stress hat starke Auswirkungen auf Einsatzkräfte in der Reaktionsphase, in der sie durch IKT unterstützt werden können.

► *Increasing Public Security by ICT-support in stress situations*

Major incidents, e.g., a chemistry accident or a major fire stipulate extreme requirements for the human ability to work under pressure, for the interface between humans and technology, and for the technology itself. Due to the strained and often stressful situation, necessary arrangements of the first responders are particularly error-prone; they require time and distract attention from the actual task. In the context of ICT-support in public security different approaches can be applied to facilitate appropriate reactions to major incidents. Stress strongly influences first responders in the reaction phase, where ICT can offer support.

Max Mühlhäuser, Dirk Bradler, Melanie Hartmann, Ralph Bruder • Öffentliche Sicherheit bezeichnet – vereinfacht gesagt – alle Maßnahmen, die das öffentliche Leben vor erheblichen Störungen schützen. Ganz grob können zwei Maßnahmenbereiche unterschieden werden. Die Prävention, also die Verhinderung von Störungen bzw. die Vorbereitung darauf und die Reaktion, also die Wiederherstellung des „Normalzustandes“ nach Unfällen und Katastrophen. In allen genannten Bereichen der Öffentlichen Sicherheit nimmt die Unterstützung durch IKT zu.

1. Prävention: die verwendeten IKT-Mechanismen sind sehr divergent: physischer Schutz, Planung und Anschlagvereitelung beispielsweise benötigen spezifische IKT-Konzepte.
2. Reaktion: Dieser Bereich lässt sich in zwei Schwerpunkte gliedern:
 - a. Koordinationsunterstützung in Zentralen: Hier wird unter anderem die Mensch-Technik- und



Max Mühlhäuser

Mensch-Mensch-Interaktion in Stabs- und Leitstellen verbessert, zum Beispiel durch multimodale Bedienkonzepte und Entscheidungsunterstützungs-Software

- b. Operative Unterstützung im Feld: Ein wichtiges Forschungsfeld ist hier die Ersthelfer-Ausstattung mit Sensorik und digitaler Kommunikation.

Ergänzend zum traditionellen Verständnis der Öffentlichen Sicherheit als Kombination aus Präventions- und Reaktionsmaßnahmen wird seit einiger Zeit besonderes Augenmerk auf kritische Infrastrukturen gelegt, das sind Institutionen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen.

Fragestellungen der Öffentlichen Sicherheit müssen in den drei Bereichen Mensch, Interaktions-Schnittstelle und Technik jeweils gezielt untersucht werden. Die entwickelten Konzepte sollen in allen drei Bereichen aufeinander abgestimmt werden. Folgende Problembereiche der Reaktionsphase werden im Folgenden behandelt:

- Der Bereich „Mensch“: Umgang mit Stress und menschlicher Fehleranfälligkeit
- Der Bereich „Interaktion“ mit Fokus auf der Unterstützung im Feld: Wie können Interaktionskonzepte mit „Proaktivität“ versehen werden?
- Der Bereich „Technik“ mit Fokus auf der operativen Unterstützung im Feld: Neue Konzepte für hochgradig dezentralisierte Peer-to-Peer-Netzwerke.

Der Mensch in Stress-Situationen

Insbesondere bei Großschadenslagen sind sowohl die Rettungsleitstellen als auch die Ersthelfer vor Ort extrem belastenden Arbeitsbedingungen ausgesetzt. Wie jedoch reagiert der Mensch unter solchen Bedingungen? Hierzu liefern Untersuchungen aus der Stresstheorie wichtige Erkenntnisse.

1950 wurde der Begriff Stress erstmals von Hans Selye in medizinisch-psychologischem Kontext erwähnt: „Die Belastungen, Anstrengungen und Ärgernisse, denen ein Lebewesen täglich durch viele Umwelteinflüsse ausgesetzt ist. Es handelt sich um Anspannungen und Anpassungszwänge, die einen aus dem persönlichen Gleichgewicht bringen können und bei denen man seelisch und körperlich unter Druck steht“. Stress ist eine angeborene und

Ralph Bruder



Vorhersage der nächsten Benutzerinteraktion

Um die Benutzerschnittstelle auf die relevantesten Elemente reduzieren zu können, muss das System in der Lage sein, die nächsten Schritte des Benutzers vorherzusagen. Dazu wird aus den vergangenen Interaktionen des Benutzers ein Interaktionsmodell gelernt. Mit Hilfe dieses Interaktionsmodells wird aus den letzten Aktionen des Benutzers $a_1 \dots a_n$ (im Beispiel in Abbildung 2 die Aktionen a d c) die Wahrscheinlichkeit der nächsten Aktion a_{n+1} vorhergesagt. Dies kann z. B. mit Hilfe von Mixed Order Markov Modellen erfolgen. Diese berechnen die nächste Aktion unter Berücksichtigung von unterschiedlich vielen vorangegangenen Aktionen (im nebenstehenden Beispiel die letzten eins bis drei Aktionen).

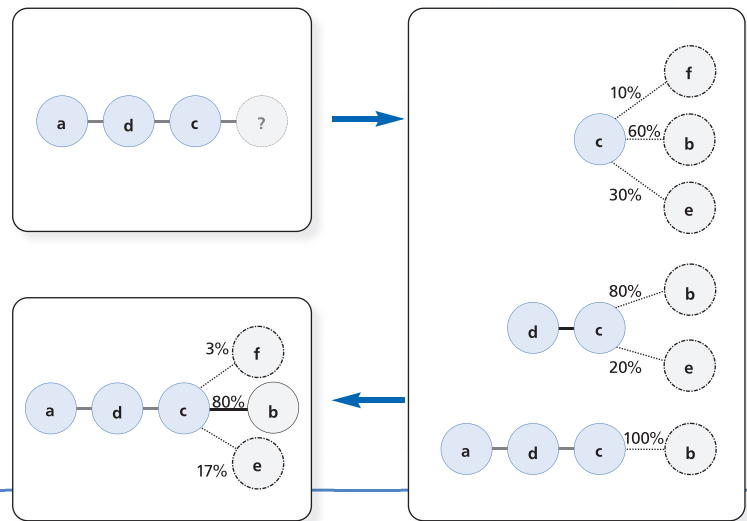


Abbildung 1
Vereinfachtes Mixed Order Markov Model unter Verwendung von Markov-Modellen erster bis dritter Ordnung und gleichen Gewichtungen.

erworbene Aktivierungsreaktion des gesamten Organismus auf Stressoren (d. h. auf alles, was das Individuum als Anforderung, Bedrohung oder Schaden bewertet). Ursprüngliches Ziel der Aktivierung war die Lebenserhaltung: Bei Gefahr kommt es zu einer raschen Bereitstellung von Energie und Kraft: Blutdruck, Adrenalin Spiegel im Blut, Herzschlagfrequenz und Atemfrequenz steigen an, innerhalb kürzester Zeit ist der Mensch kampfbereit oder fluchtbereit. Als auslösende Faktoren (= Stressoren) kommen alle inneren und äußeren Anforderungen an den Menschen in Frage. Glaubt man, eine Anforderung aktiv steuern zu können, erlebt man weniger Stress. Das Gefühl des Kontrollverlusts dagegen verstärkt die Reaktionen des Betroffenen. Überfordern die stressauslösenden Faktoren den Menschen, treten verstärkte Reaktionen auf der kognitiven (Konzentrationsstörungen), emotionalen (Angst, Wut, Verunsicherung) und körperlichen Ebene auf. Der Betroffene agiert dadurch planlos oder resigniert seine Leistung verschlechtert sich bei gleichzeitig steigender Anzahl von Fehlern. und (mittel- bis langfristig) erhöht sich seine Krankheitsanfälligkeit. Die effiziente Handlungsregulation ist unter Stress also gestört, ein vermehrtes Auftreten von Fehlhandlungen ist mög-

lich. Daraus ergeben sich besonders hohe Anforderungen an die Interaktionsgestaltung, damit Personen auch unter Stress, wie es in Großschadenslagen gegeben ist, eine optimale Leistung erbringen.

Intelligente Interaktionsunterstützung

Das Ziel intelligenter Interaktionsunterstützung ist es, Fehlhandlungen in Stresssituationen zu minimieren, dem gefühlten Kontrollverlust entgegenzuwirken und den Stress der Einsatzkräfte durch die Erstellung strukturierter und intuitiver Benutzerschnittstellen zu reduzieren. Sogenannte proaktive Benutzerschnittstellen machen dem Benutzer Vorschläge zur Interaktion statt nur auf Benutzereingaben zu reagieren. Diese proaktive Unterstützung kann die Interaktion für Einsatzkräfte in der Zentrale wie auch im Feld vereinfachen. Im Rahmen des Projekts AUGUR an der TU Darmstadt wurde eine solche proaktive Benutzerunterstützung entwickelt.

AUGUR ist in der Lage den Benutzer bei der Eingabe von Daten zu entlasten, indem es dem Benutzer Vorschläge zur Eingabe unterbreitet (siehe Abbildung 2) oder direkt Eingabefelder für den Benutzer vorausfüllt. Dadurch werden Fehlereingaben reduziert und Daten können schneller übermittelt werden. Für das Vorschlagen von Eingabedaten werden eine Reihe von vorliegenden Kontextinformationen, wie beispielsweise der Aufenthaltsort oder anwesende Personen, herangezogen. Die Zusammenhänge zwischen Kontextinformationen und benötigten Eingabedaten können entweder vormodelliert sein oder von AUGUR durch Beobachtung der Benutzerinteraktion mit der Zeit erlernt werden.

Zudem kann AUGUR durch wiederholte Nutzung erlernen, welche Elemente einer Benutzeroberfläche in einem bestimmten Kontext relevant sind. Dies versetzt AUGUR in die Lage, automatisch eine

Abbildung 2
Proaktive Eingabeunterstützung in AUGUR.

reduzierte Benutzeroberfläche mit den wichtigsten Elementen zu generieren. Dies vereinfacht die Interaktion auf mobilen Endgeräten und kann die kognitive Last des Benutzers weiter reduzieren, was in Stress-Situationen wie Großschadenslagen entscheidend ist.

Selbstorganisierende Infrastruktur

Rettungskräfte im Feld benötigen primär Zugriff auf ihre aktuellen Aufgabenstellungen, relevante Ressourcen und direkten Kontakt zu ihrem Gruppenleiter. Im Folgenden wird beispielhaft eine Anfrage an das Objekt „Bauhof“ an das dezentrale, ad-

hoc erstellte Peer-to-Peer (P2P)-Netzwerk (vgl. Abbildung 2) betrachtet.

Die beteiligten Endgeräte im Feld (z.B. innerhalb eines Fahrzeugs, in der technischen Einsatzleitung oder tragbar in Form eines PDAs) sind Teil des P2P-Netzes und können für Informationsweiterleitung (Routing), Abfragen und zur Datenspeicherung verwendet werden. Diese Kombination der Verwendungsmöglichkeiten ist als „Servent“-Konzept aus der P2P-Technologie bekannt. Servent ist ein Kunstwort, entstanden aus der Kombination der Wörter Server und Client. Nachdem das Endgerät eine Aktion des Benutzers

ANZEIGE



◁ Engineering
Your Future ▷

Steigen Sie ein in die globale Welt der Schienenverkehrstechnik

Sind Sie ein(e) erfolgsorientierter(e) Ingenieur/in und möchten an umweltfreundlichen Produkten in einem internationalen Umfeld mitarbeiten?

Ja? Kommen Sie zu uns und machen Sie mit.

Wir suchen am Standort Mannheim innovative

Entwicklungs- und Projektierungsingenieure (m/w)

der Fachrichtungen Elektrotechnik, Maschinenbau und Wirtschaftsingenieurwesen hauptsächlich für die Geschäftsbereiche Antriebstechnik, Nahverkehr und Lokomotivbau.

Ihre Anfragen und/oder vollständigen Bewerbungsunterlagen senden Sie bitte an

Karlheinz.Kelsch@de.transport.bombardier.com
oder kontaktieren uns unter 0621 / 7001-1223

Bombardier Transportation ist ein weltweit führender Hersteller von Schienenverkehrstechnik und Service Dienstleistungen. Zur Produktpalette zählen Fahrzeuge für den Stadt-, Regional-, Intercity- und Hochgeschwindigkeitsverkehr ebenso wie Lokomotiven, Drehgestelle, Antriebs-, Steuer- und Sicherungstechnik.

Aktuelle Stellenangebote finden Sie hier:
www.engineeringyourfuture.jobs oder
www.careers.bombardier.com

The Climate is Right for Trains

BOMBARDIER

Routing in P2P-Netzwerken

Verteilte Hashtabellen werden in P2P-Netzwerken genutzt um Datenobjekten eindeutige Schlüssel in einem definierten Wertebereich zuzuweisen. Dabei ist jeder Netzwerkteilnehmer für einen Teil des Wertebereichs zuständig. Durch Routingtabellen wird sicher gestellt, dass jeder Knoten innerhalb von wenigen Suchschritten erreicht werden kann. Die Anzahl der Suchschritte lässt sich in den meisten P2P-Netzwerken durch $O(\log n)$ bzw. $O(\sqrt{n})$ abschätzen. Die nebenstehende Abbildung zeigt einen Ausschnitt des P2P-Overlay Netzwerks CAN. Jeder Netzwerkteilnehmer nimmt in seiner Routingtabelle die Koordinaten des Wertebereichs und die IP-Adresse seiner direkten Nachbarn auf. Eine Nachricht wird weitergeleitet an den Nachbarn, welcher dem gesuchten Zielbereich am nächsten ist. Dieses Verfahren nennt man Greedy-Routing.

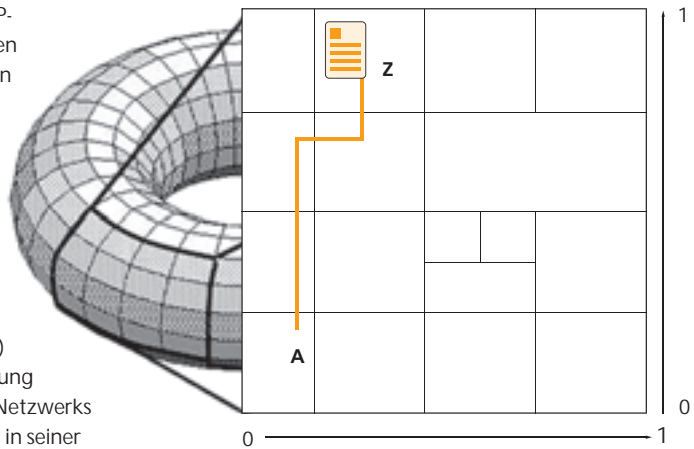


Abbildung 3
Ausschnitt des Schlüsselraumes
einer verteilten Hashtabelle.

entgegengenommen hat, z.B. durch Selektion des Objekts „Bauhof“, wird eine Route innerhalb des Netzwerkes zu dem Endgerät der dafür zuständigen Einsatzkraft gesucht. Das an der TU Darmstadt entwickelte P2P-Verfahren zur dezentralen Datenübertragung tauscht zunächst nur Routingtabellen und Basisinformationen mit anderen Geräten in Reichweite aus. In einem zweiten Schritt wird das Gerät vollständig in das Netz inte-

griert. Die Endgeräte nutzen das dezentrale und autonom arbeitende Netzwerk um Informationen zu finden oder zu veröffentlichen. Soll z.B. das Objekt „Bauhof“ aufgerufen werden, dann wird ein Pfad von dem anfragenden Endgerät zum Zielort innerhalb des P2P-Netzes gesucht. Um den gesuchten Zielort zu bestimmen, nimmt eine Funktion (z.B. die Hashfunktion SHA-1) das Schlüsselwort „Bauhof“ entgegen und generiert eine eindeutige Adresse innerhalb des Netzwerkes, diese dient als wichtigster Anhaltspunkt für die Nachrichtenweiterleitung (siehe Abbildung 3). Ist die Nachricht nach mehreren Übermittlungsschritten beim Empfänger angekommen, überprüft dieser, ob bereits Informationen über das gesuchte Objekt vorliegen und informiert den Absender. Diese nichtprobabilistische Zugriffsmethode und die dynamische Erstellung eines dezentralisierten Kommunikationsnetzwerkes erhöht die Planungssicherheit der Ersthelfer und wirkt dadurch zusätzlich stressmindernd auf die Rettungskräfte.



Max Mühlhäuser ist seit 2000 Leiter des Fachgebiets Telekooperation. Seit 2008 ist er Leiter des Arbeitsbereichs „Sichere Dienste“ des LOEWE-Zentrums CASED.



Dirk Bradler ist Leiter der Gruppe Smart Civil Security am Fachgebiet Telekooperation. Er hat 2010 seine Promotion zum Thema „P2P Concepts for Emergency Response“ abgeschlossen.



Melanie Hartmann ist Leiterin der Gruppe Smart Interaction am Fachgebiet Telekooperation. Sie hat 2010 ihre Promotion zum Thema „Context-Aware Intelligent User Interfaces“ abgeschlossen.



Ralph Bruder ist seit 2005 Leiter des Instituts für Arbeitswissenschaft an der TU-Darmstadt. Seit November 2004 leitete er als Präsident und Geschäftsführer die Zollverein School of Management and Design.

Fazit

Gerade bei Großschadenslagen muss die IKT-Unterstützung als ganzheitlicher Prozess verstanden werden, der sowohl den Menschen, die Interaktions-Schnittstelle als auch die zugrunde liegende Technik berücksichtigt. An der TU Darmstadt gelang durch die konsequente interdisziplinäre Zusammenarbeit der beteiligten Institute im vielschichtigen Bereich der Öffentlichen Sicherheit eine ganzheitliche Analyse der Problemstellung und die Entwicklung eines integrierten Lösungskonzepts mit besonderem Fokus auf der Reaktions-Phase: Das Institut für



Einsatz eines Prototyps zur digitalen Kommunikation in Katastrophenszenarien.

Arbeitswissenschaft Darmstadt analysiert die Auswirkungen von Stress-Situationen auf den Menschen. Daraus ergaben sich besonders hohe Anforderungen an die benötigten Interaktions-Schnittstellen. Das Fachgebiet Telekooperation entwickelte für diese Anforderungen kontextsensitive und lernende Benutzerschnittstellen. Sie versprechen gerade in Extremsituationen eine Entlastung der Ersthelfer und verringern die Wahrscheinlichkeit von Fehleingaben. Aus der P2P-Technologie bekannte Konzepte wurden für die kurzfristige Erstellung eines hochdynamischen und verteilten Netzwerkes am Ort der Großschadenslage verwendet. Dadurch wird digitale Kommunikation ermöglicht und die Planungssicherheit erhöht.

Fachgebiet Telekooperation

Prof. Dr. rer. nat. Max Mühlhäuser
Tel. 06151/16-70922
E-Mail: max@informatik.tu-darmstadt.de

Dr. rer. nat. Dirk Bradler
Tel. 06151/16-6702
E-Mail: bradler@tk.informatik.tu-darmstadt.de

Dr.-Ing. Melanie Hartmann
Tel. 06151/16-4752
E-Mail: melanie@tk.informatik.tu-darmstadt.de
www.tk.informatik.tu-darmstadt.de

Institut für Arbeitswissenschaften der TU Darmstadt (IAD)

Prof. Dr.-Ing. Ralph Bruder
Tel. 06151/16-2987
E-Mail: bruder@iad.tu-darmstadt.de
www.arbeitswissenschaft.de

Sicherheitskultur

für eine digitale Welt

Durch rein technische Maßnahmen lässt sich Sicherheit nicht gewährleisten, weil die Schutzziele untereinander konfliktieren und in ihrer Priorisierung unter den Nutzern technischer Systeme ausgehandelt werden müssen. Das kulturelle Erfordernis zielt auf die Aufklärung der Nutzer sowie die Bereitstellung technischer Infrastrukturen, welche die hierfür notwendigen Informationen während der Mensch-System-Interaktion liefern und flexible Lösungen als Ergebnis der Aushandlungsprozesse erlauben.

► *A Culture of Security for a Digital World*

Security can not only be guaranteed through technical devices for reasons of conflicting protection objectives, whose prioritization must be bargained by the users of technical systems. The cultural requirement aims at the education of users and at providing the technical infrastructure that generates the required information during the User-System-Interaction and enables flexible solutions as a result of the bargaining-process.

Christoph Hubig • Seit der neolithischen Revolution wurde in Ablösung der „Zufallstechnik“ (José Ortega y Gasset) der Jäger und Sammler die Planbarkeit des Handlungserfolgs dadurch sichergestellt, dass den Gefahren der Natur durch den Aufbau technischer Systeme und Infrastrukturen begegnet wurde. Gefahren wurden transformiert in Risiken, die gestaltbar und wählbar wurden: Sicherheit als „Freiheit von unakzeptablen Risiken“ (ISO/IEC/TÜV). Wenn es ein Spezifikum der Technik gibt, so scheint dies Sicherheit als störungsfreie Wiederholbarkeit zu sein. Sicherheitsdefizite erscheinen als genuin technische Herausforderungen. Wozu bedarf es hier einer „Kultur“?

Sicherheitskonzepte

Sicherheit als „Schutz vor ...“ und Sicherheit als „Sicherung des Gelingens zu ...“ sind zu unterscheiden. Beides scheint durch Technik leistbar: Die immer komplexer werdenden technischen Systeme bis hin zu denjenigen einer „digitalen“ Welt dienen der Gefahrenabwehr und eröffnen neue Optionen gelingenden Handelns. Web 2.0 und Ubiquitous Computing, Smart Cards und elaborierte Telekommunikation erlauben die Minderung und Minimierung von Risiken (z. B. qua Vermeidung medizinischer Fehldiagnosen, Kompensation physischer und kognitiver Einschränkungen und Infor-

mationsdefiziten, Optimierung der Prävention) und erweitern unsere Handlungsräume (z. B. durch intelligente Seniorenwohnungen, Blindennavigation, smart factory, child finder, effektives Katastrophenmanagement). Assistenzsysteme sollen unser Leben leichter, angenehmer machen; Widerständigkeiten sollen abgebaut und die Lebensführungsumstände individueller und situationsadäquater anpassbar werden. Hierin liegen die Chancen durch die komplexen Systeme einer digitalen Welt. Gleichwohl besteht aus guten Gründen seit den 80er Jahren des letzten Jahrhunderts eine Diskussion um eine Sicherheit „vor“ den durch die Systeme ermöglichten Effekten. Man untersucht Risiken, die im Zuge der Nutzung der Systeme entstehen, und entwickelt Strategien ihrer Minderung. Hierbei zeigen sich ganz unterschiedliche Schutzziele und zahlreiche Binnenkonflikte zwischen den Beurteilungskriterien, bedingt durch unterschiedliche Interessen von Nutzern, Diensteanbietern und Betreibern. Neben „technikimmanenten“ Kriterien einer Safety wie Ausfallsicherheit/Zuverlässigkeit und Funktionssicherheit/Fehlertoleranz (für System und Systemnutzung), unter denen Versagens- und Betriebsrisiken minimiert werden, heben die Security-Schutzziele ab auf Vertraulichkeit, Integrität/Entdeckbarkeit von Fälschungen, Anonymität/Unbeobachtbarkeit/Unverkettbarkeit, Zurechenbarkeit/Authentizität sowie Verfügbarkeit.

Sicherheitskultur

Eine solchermaßen gefasste Sicherheit verweist auf die Notwendigkeit der Einbettung in eine Sicherheitskultur: Erstens bedarf es eines Abgleichs der zu vermeidenden Risiken, der Schutzziele einer Sicherheit vor systemischen Effekten (der Systeme selbst und/oder ihrer fehlerhaften oder missbräuchlichen Nutzung) mit den wachzunehmenden Chancen einer „Sicherung zu ...“. Zahlreiche Dienstleistungen erfordern eine Profilierung der Nutzerinnen und Nutzer, um adäquat vollzogen werden zu können. Sicherheitsstandards lassen sich in etlichen Fällen nur durch Überwachung erfüllen. Privacy konfliktiert also mit Transparenz. Zweitens zeigen die Charakteristika einer Security, dass je nach Nutzerintentionen Vertraulichkeit, Integrität, Anonymität, Zurechenbarkeit und Verfügbarkeit bezüglich ihrer Gra-

Christoph Hubig



duierung und Priorisierung problemadäquat und flexibel auszuhandeln sind.

Die Frage eines umfassenden Diskussionsrahmens von Sicherheitskultur erscheint in ihrer Dringlichkeit.

Probleme und Forderungen

Angesichts der Missbrauchsmöglichkeiten (von der Überwachung bis hin zu Aktivitäten der „Cypher-Punks“ als „Piraten des 21. Jahrhunderts“ auf der Gegenseite) dürfen sich unaufgeklärte Nutzerinnen und Nutzer nicht mangels Wissen über die Leistungsfähigkeit der Schutzmechanismen in falscher Sicherheit wiegen oder überfordert werden angesichts technischer Optionen etwa der Verschlüsselung und Kryptographie. Ein naiver Optimismus bezüglich neuer Freiheiten universeller Informiertheit oder einer umfassenden Lebenserleichterung darf die Orientierung nicht vereinsamen. Denn über den Verlust der Widerständigkeit im Zuge der Delegation von Leistungen an die Systeme verlieren wir in demselben Maße Kompetenzen (die wir bei Systemausfall vermissen), wie wir unsere Handlungsräume erweitern und unser Leben angenehmer machen.

Gewiss: Elaborierte Techniken des Datenschutzes sind bereitgestellt, z. B. zur Minimierung und systematischen Vermeidung von Datenspuren beim Web-Zugriff und Web-Kommunikation. Was nutzt dies jedoch, wenn die Nutzerinnen und Nutzer die elaborierten Techniken der Anonymisierung und Pseudonymisierung mangels technischem Know-how nicht nutzen (können), und aus derselben Liga der Informatik-Genies, die diese Entwicklungen vorantreiben, auch diejenigen stammen, die sie überwinden und missbrauchen können? Und was nutzen technische Optionen zur Herstellung von Transparenz, zur Bereitstellung von Ausstiegspunkten oder zur Integration in Netzwerke zwecks Lebenshilfe, Unterhaltung, Accident-Management oder Katastrophenschutz, wenn eine sorgfältige Analyse über die Notwendigkeit oder Zulässigkeit oder ein Verbot der Zusammenführung von Daten dem Einzelnen seine Rechte und Pflichten nicht problematisiert, sondern zugunsten eines diffusen Systemvertrauens außen vor bleibt? Was nutzt ein effizientes technisches Arsenal für den Katastrophenschutz, wenn das menschliche Engagement bei Systemversagen nicht mehr auf ur-

spprüngliche Kompetenzen zurückgreifen kann? Oder zu Ungunsten persönlicher Fürsorge die Verantwortung für die Alten an die intelligente Seniorenwohnung delegiert wird? Was erbringen Abwägungen über Zulässigkeit oder Unzulässigkeit der Kryptographie angesichts behördlicher Sicherheitsdesiderate, wenn im Falle der Prohibition gilt: „Dann haben eben nur die Verbrecher Kryptographie!“ Von einer Privatsphäre ganz zu schweigen, die angesichts der technischen Möglichkeiten nur noch derjenige für sich reklamieren kann, der uninteressant ist, analog der einzig noch durch Off-line-Betrieb zu realisierenden Sicherheit relevanter Rechner.

Lösungskonzepte

Fragen über Fragen. Patentrezepte zu ihrer Beantwortung stammen oft von gut meinenden Propagandisten, die angesichts der Deinstitutionalisierung des Netzbetriebs und eines individuell adaptiven Ubiquitous Computing klassisches institutionelles Handeln des Verbraucherschutzes und der Überwachung („Zensur“) rehabilitieren wollen.

Konkrete Lösungen lassen sich m. E. nur durch Verfahren etablieren, die Mensch-System-Interaktionen kritisch zu begleiten erlauben. Interaktion beruht ja auf „Erwartungserwartungen“: Erwartungen der Nutzer über Erwartungen des Systems über deren Erwartungen und umgekehrt. Ein Abgleich solcher Erwartungen als notwendige Bedingung von Sicherheit sollte bei neuen Entwicklungen erstens im Vorfeld in Gestalt von organisierten Entwickler – Nutzer-Dialogen stattfinden. Zweitens muss parallel zur Nutzung eine Kommunikation über die Nutzung im Dialog zwischen (Assistenz-)System und Nutzer möglich sein: Herstellung von Transparenz on demand über Systemstrategien, Risiken, Bedingungen gelingender Nutzung, Gründe für Misserfolg, Verlautbarung und/oder Empfehlungen von Ausstiegspunkten. Drittens sollte ein institutionalisierter Erfahrungs-



Christoph Hubig ist seit 2010 Professor an der TU Darmstadt. Er leitet das Fachgebiet Philosophie der wissenschaftlich-technischen Kultur im Fachbereich Gesellschafts- und Geschichtswissenschaften.

austausch über die Nutzung in entsprechenden www-Foren stattfinden: Hier sollte die Einhaltung von Security-Kriterien bilanziert, Vereinseitigungen abwägend relativiert und Lernerfolge gezeitigt werden jenseits doktrinäer Aufklärung oder anonymer Vergemeinschaftung, hintergründiger Adaptivität der intelligenten Systeme oder einer Verwiesenheit auf individuelle, isolierte eigene Erfahrungen.

Medienkompetenz wird, wie alle Kompetenzen, nicht über Wissensvermittlung erreicht, sondern durch empfehlungsgeleitetes Training in Abarbeitung an Widerständigkeit. Sicherheit, die jegliche Widerständigkeit abzubauen sucht, zerstört Kompe-

tenz und verhindert die Herausbildung neuer Kompetenzen. Mit Blick auf die biedermeierliche Empfehlungs- und Beratungskultur der Salons, Zirkel und Gesellschaften angesichts der Herausforderungen der ersten industriellen Revolution ist auch für uns eine Art neues „Biedermeier“ zu fordern, damit Systemvertrauen entstehen kann.

Institut für Philosophie
 Prof. Dr. Christoph Hubig
 Tel. 06151/16-64511
 E-Mail: hubig@phil.tu-darmstadt.de
www.philosophie.tu-darmstadt.de

ANZEIGE

Konstruktive Wege für die Zukunft finden – mit JOST.



JOST ist eine internationale Unternehmensgruppe, die verbindet. mit unseren Sattelkupplungen, Stützwinden, Auflieger- und Containertechnologien und Zwangslenkungssystemen geben wir seit 1952 sicheren Halt auf den Wegen in die Zukunft. Heute gehören wir – dank über 2.000 Mitarbeitern in 25 Niederlassungen und Produktionsstandorten auf allen Kontinenten – zu den weltweit führenden Unternehmen der Branche. Dabei zeichnen wir uns durch Flexibilität, technisches Können, unternehmerisches Handeln und eine gelebte Verbundenheit zu unseren Mitarbeitern aus. Werden Sie ein Teil unserer Erfolgsgeschichte, und meistern Sie ihre Herausforderung als:

Trainee zum Qualitätsingenieur Lieferantenentwicklung (m/w) in China bzw. Indien

Aufgabengebiet:

- Qualitätsvorausplanung der Kaufteile mit den Lieferanten
- Auditieren von Lieferanten
- Reklamationsbearbeitung von Kaufteilen
- Vereinbarung und Kontrolle von Verbesserungsprogrammen mit den Lieferanten

Zusätzliche Informationen:

An unserem Standort in Indien oder China lernen Sie zunächst das Unternehmen JOST und die Abläufe vor Ort kennen. In der zweiten Phase des Traineeprogramms erfahren Sie in unserem Headquarter in Neu-Isenburg mehr über die JOST Produktpalette, unsere Produktionsabläufe, unsere Mitarbeiter, Lieferanten und Kunden. Im Training on the Job wachsen Sie, unterstützt von erfahrenen Kollegen, in Ihren zukünftigen Aufgabenbereich hinein. Zusätzlich erhalten Sie fachspezifische Schulungen, um Sie auf Ihre zukünftigen Aufgaben vorzubereiten.

Anforderungen:

- Sehr gut abgeschlossenes technisches Hochschulstudium
- Idealerweise erste Kenntnisse im Bereich Qualitätsmanagement/-sicherung in der Automobil(zulieferer)industrie
- Verhandlungssichere Englisch- und Deutschkenntnisse sowie sehr gute Kenntnisse in Hindi oder Chinesisch
- Hohe Reisebereitschaft, Flexibilität und Verantwortungsbewusstsein
- Teamgeist und analytische, zielorientierte Arbeitsweise

Ihr Weg beginnt hier – mit einer aussagekräftigen und vollständigen Bewerbung, unter Angabe Ihres Gehaltswunsches, über unser Online-Bewerbungsportal: <http://www.jost-world.com/karriere/arbeiten-bei-jost.html>

JOST-Werke GmbH | Siemensstraße 2 | 63263 Neu-Isenburg | Ihr Ansprechpartner: Frau Fee Schulmeyer Telefon: 06102 295-265 | www.jost-world.com



Inserentenverzeichnis

AVL www.avl.com	Seite 53	Omya International AG www.omya.com	Seite 35
Bombardier Transport GmbH www.bombardier.com	Seite 75	Procter & Gamble www.pg.com	Seite 52
Daimler AG www.daimler.de	Seite 29	Rhode & Schwarz www.rohde-schwarz.de	Seite U2
European Space Agency (ESA) www.esa.int	Seite 21	SCHENCK Process GmbH www.schenckprocess.com	Seite 38
Jost Werke GmbH www.jost-world.com	Seite 81	Siemens AG Energy Sector, Erlangen www.siemens.com/energy	Seite 23
KNF Neuberger GmbH www.knf.de	Seite 63	Siemens AG GSS, Nürnberg www.siemens.com/careers	Seite U4
KSB Aktiengesellschaft www.ksb.de	Seite 71	Software AG www.softwareag.com	Seite 26
Lufthansa Training & Conference Center Seeheim www.lufthansa-seeheim.de	Seite 49	stellenwerk www.stellenwerk-darmstadt.de	Seite U3
MAINOVA AG www.mainova.de	Seite 6	Wissenschafts- und Kongresszentrum www.darmstadtium.de	Seite 11

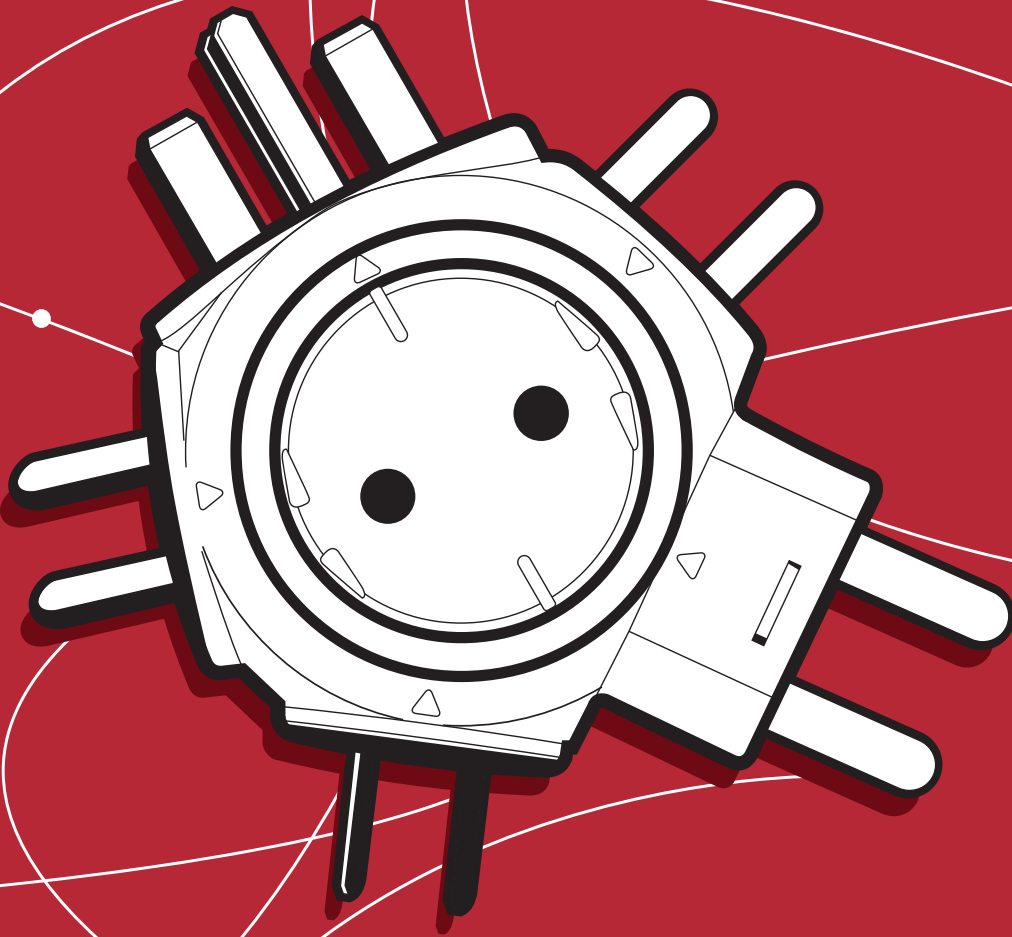
Bildnachweise

Titel und Porträts: Katrin Binner, S. 14/T. Ackermann, S. 22/J. Rodrigues Henriques, S. 35/J. M. Renes, S. 41/S. Mühlbach/M. Stöttinger, S. 45/F. Armknecht, S. 49/M. Steinebach/M. Schneider, S. 55/D. Heinson/M. Bedner, S. 59/A. Buchmann, S. 65/E. Bodden/L. Patzina/S. Patzina/A. Sewe, S. 76/D. Bradler/M. Hartmann/R. Bruder: privat, S. 18: Business Risk & Crisis Management GmbH (Abbildung 1), S. 20: ProSTEP iViP (Abbildung 3), S. 34: Andreas Buhr (Abbildung 1), S. 68 und 69: Heiko Spies (Abbildungen 1 und 2), S. 70: Richard Gay (Abbildung 3), S. 77: Mit freundlicher Genehmigung der Feuerwehr Darmstadt.
Alle sonstigen Schaubilder und Grafiken: CASED.

Impressum forschen 2/2010

Herausgeber: Der Präsident der TU Darmstadt,
Prof. Dr. Hans Jürgen Prömel
Fachliche Beratung: Dr. Christiane Ackermann, Leiterin Dezernat Forschung
Redaktion: Jörg Feuck, Leiter Corporate Communications
Koordination der Autoren: Anne Grauenhorst, CASED

Verlag: vmm wirtschaftsverlag gmbh & co. kg
Maximilianstraße 9, 86150 Augsburg
Gestaltung und Produktion: conclouso, Mainz
Druck: AZ-Druck, Kempten
Auflage: 6000



> EIN JOB PASST IMMER ...

Jobs, Praktika, Stellen:
Hier findest Du alles!

Viele neue Angebote jeden Tag –
für Studierende, Absolventinnen und Absolventen.

Finde Deinen Job auf
www.stellenwerk-darmstadt.de

stellenwerk

*das Jobportal
der TU Darmstadt*



**Jetzt
neu!**

studenten**werk**darmstadt



TECHNISCHE
UNIVERSITÄT
DARMSTADT