ITG news
INFORMATIONSTECHNISCHE GESELLSCHAFT IM VDE
01/2014

# Kann die IKT absolut sicher sein?

In dieser ITG-News haben wir einen Schwerpunkt auf den Bereich der Informations- und Kommunikationssicherheit gelegt. Bereits seit über einem Jahr hat Herr Prof. Kays von der Universität Dortmund und Vorstandsmitglied der ITG die Aufgabe übernommen, ein Fokusprojekt zu diesem Thema in der ITG aufzubauen. Die Arbeit ist weitgehend abgeschlossen; eine erste größere Aktivität der Fokusgruppe, die unter dem Namen „Fresco – Future Reliable and Secure Communications“ arbeitet, wird am 25.02.2014 ein Workshop zum Thema „Zuverlässige und sichere Kommunikation“ in der Vertretung der Bayerischen Landesregierung in Berlin sein. In diesem Workshop sollen die Fragen der IT- und Kommunikationssicherheit und ihre Auswirkung auf zukünftige Anwendungsfelder wie Industrie 4.0, Smart City, intelligente Transportsysteme und Logistiksysteme diskutiert werden.

Neue Kommunikationstechnologien öffnen auch neue Tore für Angriffe.

Genau mit diesen Fragestellungen beschäftigen sich auch vier Beiträge dieser ITG-News, die zeigen, wie komplex und schwierig die Themen- und Problemstellungen sind, wenn verbesserte Sicherheitslösungen erarbeitet werden sollen. Durch die schnelle Einführung immer neuer Kommunikationstechnologien wie des iPhones und den damit ermöglichten Applikationsprogrammen werden laufend neue Tore für Angriffe auch in sensiblen Bereichen wie der Industriesteuerung oder dem künftigen Smart Grid geschaffen.

Hardware- und Software-basierte Sicherheitstechniken, wie sie im ersten Beitrag des Schwerpunkts diskutiert werden, könnten neue Möglichkeiten bieten. Wie schwierig die Fragestellungen zur sicheren Übertragung von Informationen in Netzen sind und wie durch kryptographische Methoden versucht werden kann, die bestehenden Sicherheitsprobleme zu überwinden, beschreiben der zweite und der

dritte Beitrag dieser Ausgabe. Sie zeigen aber auch die Probleme und Grenzen auf, die selbst bei Anwendung hochintelligenter Verfahren noch bestehen. Der vierte Beitrag diskutiert die Grundrechte und den Datenschutz besonders unter dem Aspekt der Einbettung der technischen Strukturen in ein internationales Umfeld. Insgesamt ist es dem Redaktionsbeirat und vor allem den Autoren gelungen, mit den publizierten Aufsätzen einen hochinteressanten Beitrag zur Diskussion der IKT-Sicherheit zu leisten.

**PROF. DR.-ING. INGO WOLFF**
ITG-Vorsitzender

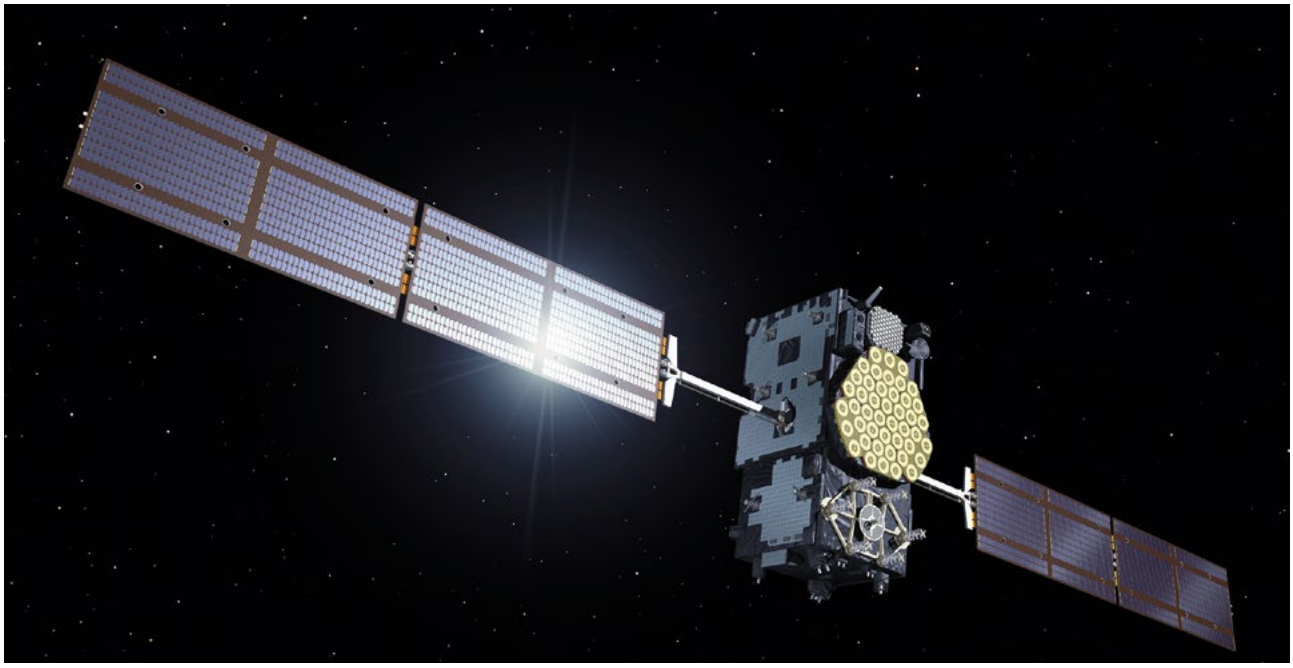
**ITG-PREISE**

# Bewerbungsfristen laufen aus

Für den ITG-Förderpreis 2014 endet am 7. Februar 2014 die Frist zur Einreichung von Vorschlägen und Bewerbungen. Mit dem Preis werden bis zu drei junge ITG-Mitglieder für besonders herausragende Dissertationen auf dem Gebiet der Informationstechnik ausgezeichnet. Jeder Preis ist mit einer Geldprämie von 2000 Euro verbunden. Eine Woche später, am 15. Februar 2014, ist Einsendeschluss für den mit 3000 Euro dotierten Preis der ITG für besonders hervorragende Publikationen auf dem Gebiet der Informationstechnik für Wissenschaftler und Ingenieure. Weitere Informationen und Einzelheiten zu den Bewerbungsmodalitäten der verschiedenen Preise der ITG unter:
**// www.vde.com/itgpreise**

## Inhalt

**Meldungen** 02
**Themenschwerpunkt**
IT-Security and Privacy 08
**Bericht**
ITG-Preisverleihung 24
**Aus den Fachgremien** 26
**Termine** 28



NAVIGATIONSTECHNOLOGIE

# Künftige Wege in der Navigation: Wo geht die Reise hin?

*Auf einer öffentlichen Diskussionssitzung des Fachausschusses 7.2 „Funksysteme“ ging es um Technologietrends und Applikationen im Bereich der Navigation – von Satellitennavigationssystemen über Ortungen in Notfällen bis hin zur Logistikbranche.*

Navigation ist allgegenwärtiger Bestandteil unserer Welt – sowohl für private als auch für industrielle Anwendungen. Angesichts großer technologischer Fortschritte stehen immer neue und verbesserte Möglichkeiten für die Navigation zur Verfügung und nähren den wachsenden Bedarf neuer Applikationen. Welche Technologietrends sind in Zukunft zu erwarten? Dieser Frage widmete sich am 14. November die öffentliche Diskussionssitzung „Künftige Wege in der Navigation – wo geht die Reise hin?“, die der ITG-Fachausschuss 7.2 „Funksysteme“ zusammen mit dem Institut für Kommunikation und Navigation des Deutschen Zentrums für Luft- und Raumfahrt (DLR) veranstaltete. Die Organisatoren Prof. Uwe-Carsten Fiebig und Prof. Michael Meurer stellten ein spannendes Vortragsprogramm zusammen, das den vielfältigen Navigationstechnologien Rechnung trug.

Wie Prof. Fiebig in seinem Übersichtsvortrag zu Beginn der Veranstaltung betonte, wird die Zusammenführung unterschiedlicher Navigationstechnologien an Bedeutung gewinnen: In einigen Jahren werden zusammen über 100 Satelliten von vier weltweit operierenden Navigationssystemen die Erde umkreisen. Der gleichzeitige Empfang von Signalen dieser Systeme wird Standard. Für eine durchgängige Navigation auch dort, wo Satellitensignale nur schlecht oder gar nicht empfangen werden, ist die Multisensornavigation zur Stelle: Die Satellitennavigation wird durch terrestrische Funksignale (WLAN, Mobilfunk, proprietäre Systeme), Inertial- und andere Sensoren, Karten sowie Kameras ergänzt.

## GPS, GLONASS und Beidou

Der Aufbau des europäischen Satellitennavigationssystems Galileo ist weitgehend im Zeitplan. Herr Bernhard kleine Schlarmann (ESA) zeigte anhand erster Messergebnisse, dass Galileo eine beeindruckende Performance erzielen wird. Ferner skizzierte er die Modernisierung von GPS und GLONASS (des amerikanischen bzw. russischen Satellitennavigationssystems) und berichtete über den Aufbau des chinesischen Systems Beidou. Sämtliche Satellitennavigationssysteme werden mehrere Signale verwenden, die verschiedenen Diensten dienen. Der neue Mobilfunkstandard LTE unterstützt die Lokalisierung durch spezielle „positioning reference signals“. Herr Graf (Huawei) stellte verschiedene Methoden zur endgeräte- und netzwerkseitigen Lokalisierung vor. Das bereits heute eingesetzte, aber noch relativ ungenaue Cell-ID-Verfahren könnte bald durch weit bessere Verfahren wie TDOA (time difference of arrival) abgelöst werden. Dass die Navigation innerhalb von Gebäuden in besonderem Maße durch Inertial- und Magnetfeldsensoren profitiert, stellte Herr Dr. Robertson (DLR) in seinem spannenden Vortrag dar. Anhand anschaulicher Videos zeigte er, wie sich mittels SLAM (simultaneous localisation and mapping) gleichzeitig Ort und Karte elegant schätzen lassen. Herr Robertson führte aus, dass die echtzeitfähige Technologie bereits erfolgreich in großen Gebäudekomplexen funktioniert und zur Navigation

für Fußgänger ausreichend hohe Genauigkeiten liefert.

In Zukunft wird die Satellitennavigation auch sicherheitskritische Anwendungen unterstützen. Daher kommt der Integrität und Robustheit der Satellitennavigation eine große Bedeutung zu. Herr Prof. Meurer (DLR) zeigte eindrücklich, vor welchen Herausforderungen und Bedrohungen sicherheitskritische Anwendungen stehen und mit welchen Maßnahmen ihnen begegnet wird. Dazu gehören bodengestützte Ergänzungssysteme sowie Empfänger mit intelligenten Antennen und Verfahren, die autonom die Integrität von Satellitennavigationssignalen beurteilen können.

Im Anschluss unterstrichen Herr Kreher (DFS) und Herr Hoppe (WSV) die Bedeutung der Navigation für die Luft- bzw. Schifffahrt und präsentierten die langfristig angelegten Roadmaps der Satellitennavigation für diese Verkehrsträger. Eine Besonderheit dabei spielen die langen Zertifizierungsprozesse, die weltweite Harmonisierung sowie Kosten und Langlebigkeit der Verkehrsträger.

In Notfällen ist die Lokalisierung auch dann notwendig, wenn der Verunglückte nicht mehr aktiv seine Position kundtun kann. Sehr anschaulich erklärte Herr Prof. Reindl (Uni Freiburg), wie man Handys mittels Mobilfunk metergenau ortet, und zeigte anhand zahlreicher Experimente, dass die Ortung auch dann gelingt, wenn das Endgerät tief unter Schutt eingeschlossen ist. Alternativ kann man auch Bio-Radar einsetzen, das im THz-Bereich arbeitet und einen Verschütteten anhand von Signaturen der Atmung erkennt. In der Logistik gibt es sehr hohe Genauigkeitsanforderungen unter oft ungünstigen Randbedingungen, insbesondere in unübersichtlichen Lagerhallen und auf großen Containerterminals: Herr Dr. Gulden (Symeo) stellte Techniken vor, bei denen proprietäre, breitbandige Funksysteme die Satellitennavigation ergänzen und innerhalb wie auch außerhalb von Gebäuden beeindruckende Genauigkeiten erzielen. Schließlich richtete Herr Prof. Steinbach (TU München) einen weiteren Blick in die Zukunft: Mithilfe visueller Navigation in Verbindung mit Bild- und Merkmalsdatenbanken soll man künftig im Indoorbereich hervorragend navigieren und gleichzeitig Mehrwertdienste nutzen können. Herr Steinbach kündigte dazu einen Großversuch im Deutschen Museum für den Sommer 2014 an.

Die Begeisterung für die neuen Möglichkeiten trug durch die gesamte Veranstaltung, in der eine rege Diskussion über die künftigen Wege der Navigation entstand. Herr Fiebig schloss die Tagung mit der Empfehlung, auch unseren eigenen Orientierungsfähigkeiten zu vertrauen, um nicht immer auf das Smartphone angewiesen zu sein.

**PROF. DR. UWE-CARSTEN FIEBIG**
Head of Department Communications Systems
Deutsches Zentrum für Luft- und Raumfahrt e.V.

**ECHTZEIT 2013**

# Höchste Sicherheitsanforderungen

*Die Fachtagung des Fachausschusses 6.2 „Echtzeitsysteme“ am 21. und 22. November in Boppard am Rhein hatte das Leitthema funktionale Sicherheit. Daher standen Sicherheitstechnologien und die Normungsarbeit im Mittelpunkt.*

Programmierbare elektronische Systeme werden in einer Fülle sicherheitsgerichteter Anwendungen eingesetzt. Weil falsch erstellte Systeme schwere Schäden verursachen oder gar Menschenleben gefährden können, müssen solche eingebetteten Systeme hohe Sicherheitsanforderungen erfüllen. Der industrielle Bedarf an sicherheitsgerichteten, programmgesteuerten Systemen ist hoch und steigt durch die zunehmende Automatisierung von Prozessen kontinuierlich weiter an. Im Einklang damit wächst auch das gesellschaftliche Sicherheitsbewusstsein. Dies sind die Gründe, warum die Fachtagung „Echtzeit“ in diesem Jahr das Leitthema funktionale Sicherheit aufgegriffen hat.

Normen sind für die funktionale Sicherheit von besonderer Bedeutung. Um Einblick in die Denkweise der Sicherheitstechnik sowie die Normungsarbeit zu geben, konnte es keinen geeigneteren Referenten für den eingeladenen Vortrag geben als Dipl.-Ing. Ingo Rolle. Innerhalb der Deutschen Kommission Elektrotechnik Elektronik Informationstechnik betreut er seit rund zwei Jahrzehnten die einschlägigen Gemeinschaftskomitees „Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben“ und „Funktionale Sicherheit elektrischer, elektronischer und programmierbarer elektronischer Systeme zum Schutz von Personen und Umwelt“.

Die regulären Vorträge der Tagung befassten sich mit Werkzeugunterstützung der Prüfung sicherheitsgerichteter Software auf Normenkonformität, Aspekten funktionaler Sicherheit programmierbarer elektronischer Systeme in der Automobiltechnik und mit Ansätzen zur Entwicklung sicherheitsgerichteter Systeme sowie zu ihrer Verifikation und Validierung.

Seit Langem ruft der Fachausschuss Studierende auf, ihre Abschlussarbeiten zu einem jährlichen Graduiertenwettbewerb einzureichen. Die drei Sieger erhielten nicht nur Preise, sondern auch Gelegenheit, sich und ihre Arbeiten auf der Tagung zu präsentieren.

Der Tagungsband ist im Springer-Verlag sowohl gedruckt als auch elektronisch (DOI: 10.1007/978-3-642-33707-9) erschienen.

**PROF. DR. DR. WOLFGANG A. HALANG**
Leiter des Fachausschusses 6.2

INTELEC®2013

# A very great success

*The 35th International Telecommunication Energy Conference INTELEC® 2013 took place from 13th to 17th October 2013 in the Congress Center Hamburg with a very great success by all attendees, connected with an excellent technical exhibition for energy powering in the telecommunication and datacenter area.*

The INTELEC® 2013 with the topic „smart power and efficiency" was organized by the Information Technical Society of the VDE/ITG in cooperation with the IEEE (Institute of Electrical and Electronics Engineers) and IEEE PELS (Power Electronics Society). INTELEC® is an annual worldwide conference and forum which presents the latest developments in information communication energy systems and related power-processing devices and circuits. About 756 attendees from 56 different countries and twelve guest attendees enjoyed the partner program to this year's conference. 80 exhibitors and companies from all over the world provided new interesting displays and devices at the technical exhibition.

At the technical exhibition 80 companies provided new interesting displays and devices.

The INTELEC® 2013 conference program was opened by the Vice Chair Prof. Dr.-Ing. Norbert Graß, University of applied sciences Georg Simon Ohm Nuremberg, and featured by the General Chair Dr. Bruno Jacobfeuerborn, Director Technology of Telekom Deutschland GmbH with a key note speech called „Correlations between Telecommunications and Energy". „Without power no communication" – Dr. Jacobfeuerborn highlighted the important social and economically importance even for Deutsche Telekom, as security and reliability are getting more and more important due to growing broadband services. „Future of Business Solutions – Cloud Computing" was the topic of Dietmar Meding, Vice President of SAP.

Prof. Dr.-Ing. Hans-Peter Beck, Technical University (TU), Clausthal-Zellerfeld, and Prof. Dr.-Ing. Harald Schwarz, BTU Cottbus-Senftenberg, provided a comprehensive overview of the „Energiewende" in Germany and informed about the tremendous problems in the correlation to the disproportional energy production (Wind, Photovoltaic) with the need of energy storage for the save and solid electrical powering to the customer. Prof. Dr. Rik de Doncker, RWTH Aachen, favoured the DC-Grid for the future Energy Network to the customers' home. Both tutorials which concentrated on the Energy Storage, the big task for the near future, Fuel Cells and Batteries, were visited from 31 attendees.

144 papers were presented in several sessions concerning important topics like Power Supply, New Technologies, DC Grid, Energy Storage-Batteries (Lead-Acid, Lithium) and Fuel Cells, current worldwide activities in the standardization and safety specifications for critical infrastructure for „smart" solutions like Smart Grid and Smart Metering, Green Energy, Techno-Economics, Maintenance of Equipment and Service Concepts, Thermal Management, Disaster Recovery and Power Quality. 28 posters showed current research activities and projects in universities and laboratories worldwide. Two workshops about „Energy Storage Systems and HVDC" dealt with the latest developments in the field of energy efficient powering of central offices, the equipment of the Next Generation Network (NGN) and the datacenter with the possibility for back reflections.

Every conference day was titled with a special slogan and opened from a plenary as well as an invitation presentation in the morning. The „GREEN DAY" was opened by a plenary themed „SMARTer 2020 – ICT Driving a Sustainable Future" by Luis Neves, Vice President, Group Transformational Change & CR (GCCR) of Deutsche Telekom AG and was followed by Friedrich Wolf, Head of Business Development, EON Connecting Energies GmbH, who presented his paper „Energy, IT and Telecommunications: Interface, overlap, convergence, merger?"

A considerable social program included a Hamburg Harbour Tour, a visit of the Hamburg Container Harbour as well as a visit of the Airbus-Company, a banquet with excellent music from the Beatles and a comprehensive partner program completed this years' INTELEC. The next 36th INTELEC® 2014 will take place from 28th September to 2nd October 2014 in Vancouver, Canada themed: „Resilient Communications Energy for our Connected World".

**WILFRIED SCHULZ**
INTELEC® 2013, Member of the Program Committee

ZDN 2013

# Von SDN über Sicherheit bis zu innovativen Anwendungen

*Am 20. September 2013 fand die 12. ITG-Fachtagung „Zukunft der Netze“ in Osnabrück statt. Experten aus Industrie und Hochschulen berichteten über aktuelle Forschungstrends im Bereich der Kommunikationsnetze und -systeme.*

Die neuen und alten FA-5.2-Leiter (v.l.): Dr. Joachim Sachs, Ingo Willimowski, Prof. Christian Wietfeld und der Tagungsleiter Prof. Ralf Tönjes

Die diesjährige Tagung stand unter dem Leitthema „Application-driven Networking“. Anwendungen haben vielfältige Anforderungen bezüglich Datenrate, Zuverlässigkeit, Robustheit, Skalierbarkeit, Energieeffizienz und Langlebigkeit. Auf der Tagung wurde diskutiert, wie zukünftige Kommunikationsnetze und -systeme dieser geforderten Flexibilität gerecht werden können. So waren die Schwerpunktthemen der diesjährigen Sitzungen „Software-Defined Networking (SDN)“, „Sicherheitslösungen“ und „Netztechnologien für innovative Anwendungen“.

Eine mit äußerstem Interesse verfolgte Keynote mit dem Titel „SDN und Virtualisierung – Hype or Hope“ leitete die erste Sitzung zu diesem Thema ein. Die Vorträge zeigten das große Potenzial der SDN, warfen aber auch viele offene Fragen auf. Das Thema wurde vom Fachpublikum sehr kontrovers diskutiert – mit dem Fazit, dass das originäre SDN auf zu einfachen Annahmen basiert und weiterführende Arbeiten notwendig sind. Eine Keynote zu Energieeffizienz im Mobilfunk gab einen Überblick über Green-IT-Technologien aus aktuellen Forschungsprojekten. Die prognostizierten Zahlen für das Energieeinsparpotenzial zeigten, dass die Technologien nicht nur ökologisch, sondern auch ökonomisch bedeutend sind. Sicherheitskonzepte für zukünftige dienstorientierte Netze standen im Fokus der Sitzung Sicherheitslösungen. Die letzte Sitzung diskutierte zukünftige Erweiterungen der Netztechnologien für innovative Anwendungen. Der Fokus lag hierbei auf LTE-Erweiterungen für eine batterieschonende Maschine-zu-Maschine (M2M)-Kommunikation und der Nutzung von Device-to-Device (D2D)-Kommunikation für eine effizientere Ressourcennutzung. Zudem wurden CDN (Content Delivery Networks) analysiert und die zugehörigen Anforderungen an das zukünftige Traffic Engineering aufgezeigt. Während der Vortragspausen präsentierten aktuelle Forschungsprojekte aus dem Hochschulbereich ihre Demonstratoren.

## Deutschlandfunk berichtete

Die Fachtagung „Zukunft der Netze“ ist eine Veranstaltung des ITG-Fachausschusses 5.2 „Kommunikationsnetze und -systeme“ und wurde lokal von der Hochschule Osnabrück ausgerichtet. Der Deutschlandfunk berichtete in zwei Sendungen über die Tagung. Die über 50 Teilnehmer verschafften sich einen Überblick über aktuelle Technologien und zukünftige Entwicklungen. Und die gemütliche Atmosphäre beim gemeinsamen Abendessen am Vorabend der Tagung in der Osnabrücker Altstadt ermöglichte es, persönliche Kontakte zu vertiefen.

Am Vorabend der vom FA 5.2 organisierten Tagung wurde Dr. Joachim Sachs, Ericsson, als Nachfolger des langjährigen FA-Leiters Ingo Willimowski, Vodafone, gewählt, der gemeinsam mit Prof. Christian Wietfeld, TU Dortmund, die Leitung des FAs in Zukunft wahrnehmen wird.

Die Präsentationen der Tagung können unter der Seite www.vde-itg-kommunikationsnetze.de/veranstaltungen/zdn2013.html heruntergeladen werden. Die nächste ITG-Fachtagung „Zukunft der Netze“ ist für den 26. September 2014 in Braunschweig geplant.

**PROF. RALF TÖNJES**
Tagungsleiter

MMBnet-2013-WORKSHOP

# Die Leistung, Zuverlässigkeit und Verlässlichkeit von Kommunikationsnetzen und verteilten Systemen bewerten

*Am 5. und 6. September fand im Fachbereich Informatik der Universität Hamburg (Arbeitsgruppe Telekommunikation und Rechnernetze) der siebte Workshop statt. Veranstaltet wurde er im Namen der GI/ITG-Fachgruppe „Messung, Modellierung und Bewertung von Rechensystemen (MMB)“.*

Kommunikations- und Rechnernetze sowie verteilte Systeme gewinnen weiterhin zunehmend an Bedeutung, z.B. in Form von sozialen Netzen, virtuellen Netzen, „Cloud Computing“-Systemen und vielen mehr – gleichzeitig nimmt ihre Komplexität erheblich zu. Besonders deutlich wird diese Tendenz bei Hochgeschwindigkeitsnetzen, dem Internet sowie bei der Mobil- und Echtzeitkommunikation. Zwar ist weiterhin eine enorme Leistungssteigerung bei der Rechnerhardware, den Vermittlungsrechnern (optische Vermittlung) und vor allem bei der Datenübertragung (sowohl bei optischer als auch bei funkbasierter Übertragung) zu verzeichnen. Andererseits steht diesen Fortschritten jedoch ein sehr starkes Wachstum bei den Benutzeranforderungen gegenüber. So gibt es beispielsweise im Kontext des Internet zurzeit die zum Teil relativ schwierig zu lösenden Probleme: Bereitstellung mobiler Internetzugänge für eine extrem hohe Anzahl von Benutzern über sehr unterschiedliche Zugangsnetze, verstärkter Wunsch nach Multimedia- und Echtzeitkommunikation, immer mehr und häufig komplexe verteilte Anwendungen bzw. anwendungsorientierte Dienste sowie eventuell gravierende Engpässe in den Anschlussnetzen und/oder den Endsystemen. Daher wird der Bedarf nach Bewertung von Kommunikationsnetzen und verteilten Systemen keineswegs überflüssig werden, sondern es werden in verstärktem Maße neue Mess-/Modellierungsmethoden und -werkzeuge erforderlich werden, unter anderem zur Berücksichtigung der Dienstgüte (QoS), des Performance-Managements und steigender Anforderungen an die Zuverlässigkeit und Verfügbarkeit.

Ziel des MMBnet-2013-Workshops sollte es deshalb sein, Weiterentwicklungen der Grundlagen und Werkzeuge zur Messung und Modellierung aufzuzeigen sowie über Erfahrungen bei interessanten Anwendungsstudien (zu Rechnernetzen oder verteilten Anwendungen) zu berichten. Gewünscht waren im Programmaufruf insbesondere auch innovative Beiträge, die eine Brücke schlagen zwischen den bislang noch häufig getrennten „Welten“ der Leistungs- und der Zuverlässigkeitsbewertung. Erwünscht war überdies eine besonders starke Beteiligung am Workshop von Nachwuchswissenschaftlern (insbesondere Doktoranden und jüngere Post Docs) mit FuE-Aktivitäten im MMB-Umfeld.

## Die Themenschwerpunkte

Für den MMBnet-2013-Workshop waren die nachfolgenden Themenschwerpunkte angestrebt worden: Bei den methodischen Grundlagen und Werkzeugen:

- Formale Beschreibungstechniken (zur Spezifikation von System-, Last- und Zuverlässigkeitsmodellen)
- Last-/Verkehrsmodellierung und -charakterisierung, Lasttransformation, „Traffic Engineering“
- Mathematisch-analytische, simulative, hybride/heterogene Modellauswertung
- Modellierungswerkzeuge für Netzanalysen, Netzemulatoren, Last-/Verkehrsgeneratoren
- Messmethoden und -werkzeuge;

Bei den Anwendungsbereichen (bezogen auf die Bewertung):

- Internet, Intranets, „Future Internet“, „Internet of Things“
- Mobilkommunikation und drahtlose Netze (u.a. MANETs, VANETs, UMTS, LTE, WLANs, Sensornetze, „Body-Area“-Netze), „Ubiquitous Computing“
- Echtzeitkommunikation (z.B. IPTV, VoIP, „Quadruple Play“, QoS- und QoE-Bewertungen)
- „Peer-to-Peer“-Anwendungen, „Service-oriented Computing“, „Grid Computing“, „Cloud Computing“, „Content-Distribution“-Netze, „Mobile Services“
- Multimediale Anwendungen (z.B. in den Bereichen E-Learning, Telemedizin, Verkehrstelematik, Videokonferenzen und Verteiltes CSCW, Video-Streaming, Video-on-Demand), Soziale Netze etc.

Die akzeptierten Beiträge sind auf drei Sitzungen verteilt worden zu den folgenden Themengebieten:

- Drahtlose Netze und Mobilkommunikation
- Analyse von Rechnernetzknoten
- Komplexitäts- und Qualitätsbewertung innovativer Internet-Anwendungen und -Architekturen.

Darüber hinaus wurden zwei eingeladene Vorträge in das Workshop-Programm aufgenommen: Ein Vortrag aus dem akademischen, universitären Umfeld (Prof. Dr. Markus Fidler, Leibniz Univ. Hannover) sowie ein weiterer Beitrag aus der Industrie (Dr. Stephan Heckmüller, SSI Schäfer Noell, Bremen). Wie bei den akzeptierten Beiträgen des Workshop-Programms haben die Organisatoren sich bei der Auswahl der beiden eingeladenen Vortragenden darum bemüht, Theorie und Praxis nicht gegeneinander auszuspielen, sondern in angemessener Weise zu kombinieren, da beide für die gegenwärtige Informatikforschung unverzichtbar sind.

Das wissenschaftliche Programm des Workshops wurde im Übrigen abgerundet durch die Präsentation von Werkzeugen wie das an der RWTH Aachen entwickelte Simulationstool openWNS sowie der an der Universität Hamburg realisierte UniLoG-Lastgenerator.

Insgesamt nahmen knapp 30 Teilnehmerinnen und Teinehmer an dem

Workshop teil, was für einen – als sehr interaktive Veranstaltung konzipierten – Workshop sehr passend war, wie die sehr intensiven, zum Teil erfreulich kontroversen und zumeist durchaus kritischen Diskussionen unterstrichen. Inhaltlich lag die Betonung des Workshops auf Leistungs- und QoS-Bewertungen von Netzen und verteilten Anwendungen, nur in geringerem Umfang fanden Zuverlässigkeits- und Verlässlichkeitsbewertungen Berücksichtigung.

## Positives Feedback

Der Workshop wurde von vielen Teilnehmerinnen und Teilnehmern als sehr gelungene Veranstaltung gewertet. In der Abschlussdiskussion wurde die Meinung vertreten, dass die nunmehr bereits längere Reihe von MMBnet-Workshops mit Fokus auf Kommunikationsnetzen und verteilten Systemen weiterhin eine Fortsetzung erfahren sollte (auch zukünftig in einem zweijährigen Turnus, in den Jahren ohne eine MMB&DFT-Haupttagung und wiederum in der Freien und Hansestadt Hamburg – der „Perle des deutschen Nordens“ bzw. dem „Tor zu der Welt“). Somit ist der achte MMBnet-Workshop für September 2015 in Hamburg vorgesehen.

Ein besonderes „Highlight“ zum Ende des MMBnet-Workshops stellte der Workshop-Epilog des Kollegen Spaniol (alias Alois Potton) mit zwei humoristischen Kurzvorträgen dar, der, wie bereits in seinem früheren Epilog anlässlich des MMBnet-2011-Workshops, auch dieses Mal wieder einen höchst erfolgreichen Angriff auf die Lachmuskulatur sämtlicher MMBnet-Teilnehmer unternahm.

Die Proceedings des Workshops wurden als Bericht Nr. 299 des Fachbereichs Informatik, Universität Hamburg publiziert; B.E. Wolfinger, K.-D. Heidtmann, (Hrsg.), FBI-HH-B-299/13. Sie sind elektronisch verfügbar (auf INFDok – dem Dokumentenvolltextserver des Fachbereichs Informatik). Jedoch ist der Tagungsband auch gedruckt kostenlos zu beziehen über die Herausgeber oder die Bibliothek des Fachbereichs Informatik der Universität Hamburg. Überdies ist – zurückgehend auf eine Initiative des Herausgebers der Zeitschrift Praxis der Informationsverarbeitung und Kommunikation (PIK), Prof. Dr. Otto Spaniol – geplant, voraussichtlich im Frühsommer 2014 (vorgesehen: die PIK-Ausgabe 2/2014), wie bereits beim MMBnet-2011-Workshop, wiederum ein spezielles PIK-Themenheft erscheinen zu lassen, das die fünf besten Beiträge des MMBnet-2013-Workshops in entsprechend überarbeiteter Form beinhalten soll. Die Vorbereitungen für dieses Themenheft sind zurzeit in vollem Gange und die Beteiligungszusagen der Autorenteams für die fünf ausgewählten Beiträge liegen bereits vor.

**PROF. DR. BERND E. WOLFINGER**
Telecommunications and Computer Networks Division, Computer Science Department, University of Hamburg

**ZuE 2013**

# Im Herzen von Dresden

*Die Fachtagung „Zuverlässigkeit und Entwurf“ fand vom 24. bis zum 26. September mit Unterstützung der Kooperationsgemeinschaft Rechnergestützter Schaltungs- und Systementwurf (RSS) der GI/GMM/ITG im Hotel Taschenbergpalais Kempinski statt.*

Das Organisationskomitee und die Ausrichter vom Fraunhofer-Institut für Integrierte Schaltungen sowie der Technischen Universität Dresden konnten auch ein abwechslungsreiches Programm mit Fachbeiträgen, eingeladenen Vorträgen, Tutorials, Postern und vielfältigen weiteren Diskussionsmöglichkeiten anbieten. Zu den herausragenden Programmpunkten gehörten dabei unter anderem die Keynotes von Hans-Jürgen Brand (Globalfoundries) zum Thema „FinFETs – die neue Herausforderung“, von Lothar Grobelny (ZMDI) zum Thema „Strukturtest für integrierte Schaltkreise“ und von Jens Lienig (TU Dresden) zum Thema „Berücksichtigung der Elektromigration im Layoutentwurf in zukünftigen Technologien“.

Für die regulären Sitzungen der Fachtagung ZuE 2013 wurden vorwiegend anwendungsbezogene Beiträge ausgewählt. Die Themenbereiche umfassten dabei Entwurfsmethodik und Eingebettete Systeme, speziell anwendungsbezogene Beiträge zu Alterungsaspekten, thermischen Effekten, Crosstalk, Analyse, Testmethoden, Diagnose und Debugging, Routing, Modellierung und Entwurfsraumexploration.

## Bestes Paper ausgezeichnet

Weiterhin wurden in einer Special Session aktuelle Forschungs- und Entwicklungsarbeiten des vom BMBF geförderten Projektes NEEDS zu Entwurfsverfahren für 3D-integrierte Systeme vorgestellt. Die Tutorials behandelten den automatisierten Analog-Entwurf in Mikro- und Nanotechnologien (Torsten Reich und Uwe Eichler von Fraunhofer IIS/EAS, Jörg Schreiter von RacyICs und Achim Graupner von ZMDI) sowie die Memristor-Technologie (Ronald Tetzlaff und Alon Ascoli von der TU Dresden). Schließlich wurde die Auszeichnung „Best Paper der ZuE 2012“ an Michael Zwerger und Helmut Gräb von der Technischen Universität München für ihren Beitrag „Verifikation des Power-Down-Modus von analogen Schaltungen“ vergeben.

**DR. MANFRED DIETRICH**
Mikroelektronische Systeme, Abteilungsleiter, Fraunhofer-Institut für Integrierte Schaltungen IIS, Institutsteil Entwurfsautomatisierung EAS

# Themenschwerpunkt IT-Security and Privacy

AN- UND HERAUSFORDERUNGEN

# Die Bedeutung der IT-Sicherheit

*Wirtschaft, Gesellschaft und Staat sind in hohem Maße von der Zuverlässigkeit und Sicherheit der hochgradig vernetzten IKT-Systeme abhängig. Am Beispiel der Sicherheitsanforderungen für die Industrie 4.0 zeigt sich die Bedeutung der IT-Sicherheit sowie die Herausforderungen für die entsprechende Forschung.*

Technologische Innovationen und die Konvergenz von Technologien werden unsere traditionellen Arbeits- und Lebenswelten nachhaltig verändern. Neue Gestaltungsmöglichkeiten für technische Systeme ergeben sich durch die Zusammenführung bislang getrennter Gebiete wie der Informations- und Kommunikationstechnologie (IKT), der Steuerungs- und Regelungstechnik, der Ortung, der Materialforschung oder auch der Physiologie (Haptik). Die Informations- und Kommunikationstechnologie nimmt hierbei eine Schlüsselrolle ein. Es entstehen neue gesellschaftliche Strukturen sowie Formen der Kommunikation, die auch neue Wege der demokratischen Partizipation, der sozialen Teilhabe oder des selbstbestimmten Lebens eröffnen. IKT ist hierbei der zentrale Innovationstreiber, jedoch stark abhängig vom Grad und der Qualität der Sicherheit. Wirtschaft, Gesellschaft und Staat sind in hohem Maße abhängig von der Zuverlässigkeit und Sicherheit der hochgradig vernetzten IKT-Systeme.

Unter dem Begriff Cyber-Sicherheit oder auch Cyber Security werden allgemein die Herausforderungen in Bezug auf die IT-Sicherheit zusammengefasst, die sich aus der Vernetzung von IKT-Systemen und den zunehmenden Abhängigkeiten von vernetzten, sicherheitskritischen Infrastrukturen ergeben. Cyber-Sicherheit beschreibt die Ausweitung der Aufgaben der klassischen IT-Sicherheit auf diese komplexen, auch mit der physischen Welt sehr stark vernetzten Systeme.

## Sichere Industrie 4.0

Am Beispiel der Sicherheitsanforderungen für die Industrie 4.0 sollen exemplarisch die Bedeutung der IT-Sicherheit sowie die Herausforderungen für die IT-Sicherheitsforschung aufgezeigt werden. In Industrie 4.0, der vierten industriellen Revolution, werden Produktions-IT und Business-IT vernetzt. IT-Systeme mit ganz unterschiedlichen Schutzmaßnahmen und Sicherheitsanforderungen werden miteinander verbunden, um Prozesse effizienter zu gestalten. Dadurch eröffnen sich jedoch neue Möglichkeiten, in Systeme einzudringen und Schäden hervorzurufen. Viren, die man von Desktop-PCs kennt, finden sich in Produktionsanlagen wieder. Maschinen werden zur Fernwartung freigegeben, ohne dass diese Zugänge ausreichend abgesichert sind.

Maschinen und Produkte werden in Industrie 4.0 zu intelligenten, cyberphysikalischen Systemen verbunden. Die Systeme müssen in der Lage sein, sich untereinander sicher zu identifizieren, Manipulationen zu erkennen und sicher miteinander zu kommunizieren. Sichere und überprüfbare Identitäten von Maschinen, der Schutz vor gefälschten und nachgemachten Produkten und die sichere Maschine-zu-Maschine-Kommunikation sind neue und wichtige Herausforderungen für die IT-Sicherheit in der Industrie 4.0. Das Internet ist das zentrale Kommunikationsmedium und Cloud Computing das zentrale Paradigma zur Erbringung kostengünstiger, standardisierter IT-basierter Dienste. Benötigt werden sichere und vertrauenswürdige Identitäten sowohl für Dienste als auch für Menschen. Dienste müssen sicher, dynamisch und über Organisationsgrenzen hinweg integrierbar sein.

Menschen, Maschinen, Produktionsanlagen, Geschäftsprozesse, Produkte und Dienste erzeugen ständig Daten. Zur Optimierung von Ressourcennutzungen und Geschäftsprozessen werden diese Daten in Realzeit zusammengeführt und effizient analysiert (Big Data). Die Daten dienen der Steuerung und Überwachung von unternehmenskritischen Abläufen, sie steuern das Verhalten von

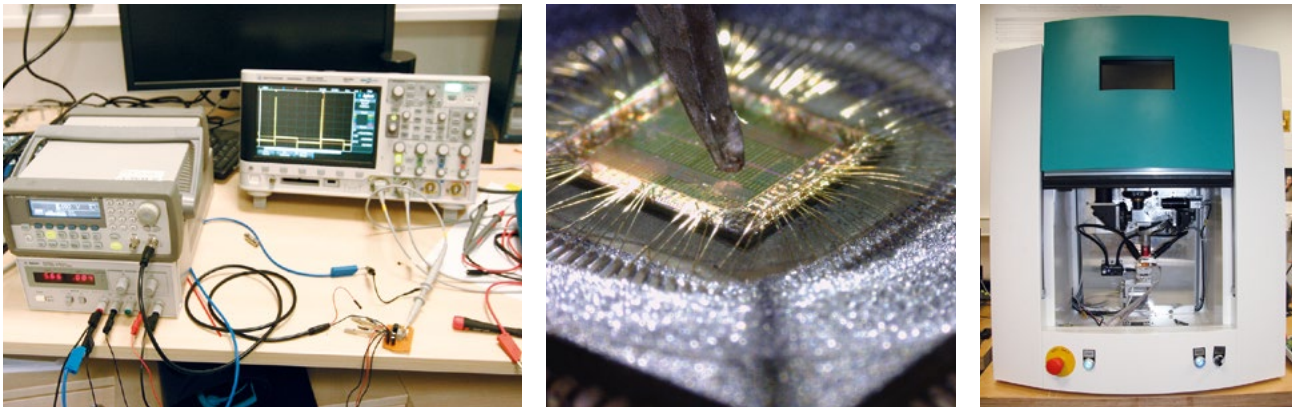


Abbildung 1: AISEC-Hardware-Labor mit Messapparaturen, EMA-Sonde und Lasermessplatz (von links nach rechts)

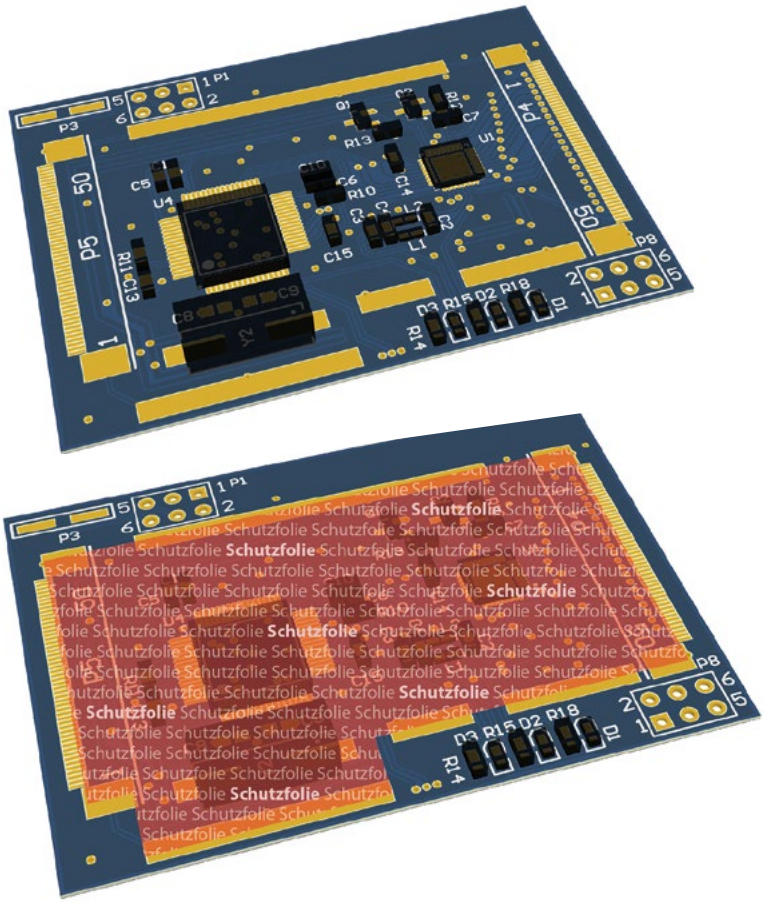



Abbildung 2: Elektronik-Bauteil (Modell oben), dessen kritische Baugruppen durch die Schutzfolie PEP (unten) geschützt werden. Bei Änderung der Folieneigenschaft wird die Firmware gelöscht.

Fahrzeugen oder auch von sicherheitskritischen Anlagen, wie Chemieanlagen. Eine gezielte Manipulation dieser Daten könnte somit verheerende Konsequenzen haben. Daten und Informationen können aber auch ein wertvolles Wirtschaftsgut sein, man denke beispielsweise an Finanzdaten oder Forschungsergebnisse, die vor unberechtigten Zugriffen und Manipulationen zu schützen sind. Zudem werden eine Vielzahl von Aufenthaltsdaten, Bewegungsprofile, Nutzungsprofile oder auch Gewohnheiten erfasst. Dies stellt eine erhebliche Bedrohung der Privatsphäre dar. Die Gewährleistung einer datenschutzbewahrenden Verarbeitung von Daten ist eine zentrale, sowohl gesellschaftliche als auch wirtschaftspolitische Aufgabe.

## Herausforderungen

Cyber-Sicherheit erfordert somit umfassende Maßnahmen, um die Korrektheit, Vollständigkeit und rechtzeitige Verfügbarkeit der Daten sowie die sichere Kommunikation und die Vertrauenswürdigkeit der eingesetzten IT-Komponenten zu gewährleisten. Sie umfasst technologische, aber auch organisatorische Maßnahmen zur Steigerung von Vertrauen in IKT-basierte Systeme und Abläufe. Erforderlich sind neue methodische und technologische Ansätze, um die Sicherheit und Vertrauenswürdigkeit von IKT-Systemen prüfbar und kontrollierbar zu erhöhen. Das mit der Nutzung der IKT-Systeme einhergehende Risiko muss methodisch erfasst und quantifiziert werden und es müssen Prozesse und Verfahren entwickelt werden, um Risiken zu minimieren und um mit den verbleibenden Risiken verantwortungsvoll umzugehen. Langfristig tragfähige Lösungen erfordern die Entwicklung neuer Sicherheits-Technologien, die die Anforderungen hochgradig, unter Umständen spontan vernetzter und eingebetteter Systeme, z.B. in Bezug auf Energie-Effizienz oder Realzeit-Anforderungen, erfüllen. Neue Sicherheitskontroll- und Schutzmaßnahmen müssen bereits frühzeitig in den Entwurf der Systeme integriert werden, um zukünftige IT-basierte Produkte und Systeme robuster und resistenter gegen insbesondere auch Internet-basierte Angriffe zu gestalten.

## Forschungsaktivitäten

Das Fraunhofer AISEC begegnet den genannten Herausforderungen mit der Entwicklung und Implementierung neuer Sicherheitstechnologien. Neben der Erarbeitung neuer allgemeiner Standards werden auch spezielle, maßgeschneiderte Lösungen für einzelne Branchen (z.B. Auto- und Zulieferindustrie), Systeme (z.B. eingebettete Systeme) und Produkte (z.B. Chips) entwickelt. Nachfolgend werden zwei ausgewählte Bereiche der Sicherheitsforschung des Fraunhofer AISEC vorgestellt: Sicherheit von eingebetteten Systemen mit dem Anwendungsfall Produktschutz sowie Mobile Sicherheit mit dem Anwendungsfall App-Analyse.

## Eingebettete Systeme

Eingebettete Systeme bestehen meist aus Baugruppe mehrerer Chips und sind im Allgemeinen über offene physische Schnittstellen leicht zugänglich. Somit sind sie Angreifern schutzlos ausgeliefert. Angreifer haben zudem die Möglichkeit, sich interne Schnittstellen, wie zum Beispiel Debug-Schnittstellen oder einen direkten Zugang zu einem integrierten Speicherchip, zu erschließen. Das AISEC verfügt über ein sehr gut ausgestattetes Hardware-Labor (vgl. Abbildung 1), mit Mehrfach-Laser-Messplätzen zur Durchführung von Fehlerinjektionen, EMA-Messplätzen, einer Kältekammer etc. Das AISEC erforscht zusammen mit industriellen Partnern neue Methoden und Werkzeuge, um die Hardware-Sicherheit von Produkten und Systemen zu analysieren und setzt die gewonnenen Erkenntnisse in innovative Lösungen um, sodass die Bausteine angriffsresistent werden.

Maschinen und Anlagen in der Industrie sind für einen langjährigen Einsatz, oft in der Größenordnung von 20 Jahren, vorgesehen. Die Migration von der heutigen Industrie 3.0 auf die nächste, von intensiver Vernetzung zum „Internet der Dinge“ geprägten Generation wird also nicht als Revolution, sondern vielmehr als Evolution stattfinden. Die Nachrüstung der Netzwerkschnittstellen von industriellen Komponenten etwa mit kryptographischen Verfahren zum Schutz des Datenaustausches ist keine Standardaufgabe. Zwar gibt es ausreichend bewährte Konzepte in der klassischen IT-Welt, diese lassen sich allerdings nicht ohne Weiteres in den industriellen Kontext übertragen. Zum einen müssen die Sicherheitslösungen mit den bestehenden Standards der Systeme kompatibel sein. Zum anderen laufen die Industriesysteme unter sehr strikten Echtzeitbedingungen. Das Zeitfenster für die Ver- und Entschlüsselung der Daten oder die Authentifizierung von Nutzern und Geräten ist äußerst klein. Am AISEC werden Sicherheitskonzepte für alle Ebenen entwickelt: Dazu zählt zum Beispiel auch ein durchgängiges Berechtigungsmanagement. Damit wird klar geregelt, wer welche Aktionen an dem jeweiligen Industriesystem vornehmen darf und kann. Neben dem Schutz vor Angriffen über das Internet muss auch die Sicherheit bei physikalischen Angriffen gewährleistet sein. Durch Verwendung von Hardware-Security-Modulen wird erreicht, dass ein System sich nicht mehr booten lässt, wenn eine manipulierte oder gefälschte Komponente in das System eingebracht wurde.

Eine elektronische Platine als Bauteil in eingebetteten Systemen bietet zahlreiche Schnittstellen für vielfältige Angriffsmöglichkeiten. Durch technische oder chemische Verfahren ist es möglich, Zugriff auf die einzelnen Bausteine auf der Platine zu erhalten und so das Zusammenwirken der Komponenten zu analysieren. Auch die Firmware lässt sich auslesen, was deren Manipulation, aber insbesondere auch deren Nachbau durch Verfahren wie das Reverse Engineering ermöglicht. Zum Schutz des in Komponenten, Systemen und Produkten enthaltenen Know-hows wird am AISEC unter anderem eine spezielle, intelligente Schutzfolie PEP (vgl. Abbildung 2) entwickelt.

Die Folie verschließt als elektronisches Siegel das Gehäuse und alle kritischen Bauteile der Geräte manipulationssicher und deaktiviert die Funktionalität des Produkts bei Siegelbruch. Im Gegensatz zu anderen Abschirmungen ist PEP auch ohne Stromzufuhr voll funktionsfähig und hält allen Angriffen stand. Die Innovation von PEP besteht in der untrennbaren Verbindung von Hardware und Schutzfolie. Die Materialeigenschaften der Schutzhülle werden als Sensoren genutzt und zum festen Bestandteil der Messschaltung gemacht. Die für die Verschlüsselung der Firmware notwendigen Schlüssel werden aus den Folieneigenschaften erzeugt und sind damit bei der geringsten Veränderung dieser Eigenschaften, wie beispielsweise Form oder Oberflächenstruktur, nicht mehr verwendbar. Jede Folie erhält bei der Herstellung einzigartige Identifikationsnummern, die für die Erzeugung einzigartiger kryptographischer Schlüssel genutzt werden. Wird eine Manipulation jeglicher Art an der Schutzfolie vorgenommen, werden Daten wie der Programmcode der Firmware gelöscht und das Gerät dadurch funktionsunfähig. Auch das Auslesen der Firmware wird damit natürlich verhindert. Durch diese Hardware-basierte Verschlüsselung in enger Verknüpfung mit einer Software-basierten, d.h. der Firmware-Verschlüsselung und durch zusätzlich verwendete Verschleierungsmaßnahmen wird ein sehr hohes Sicherheitsniveau erreicht.

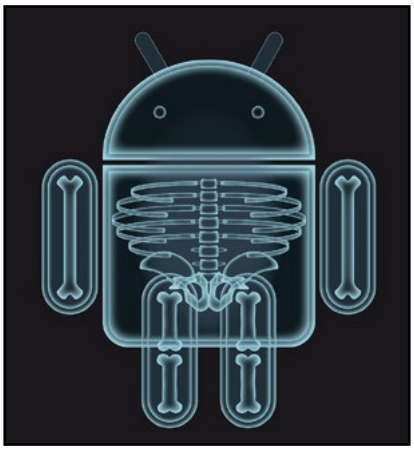
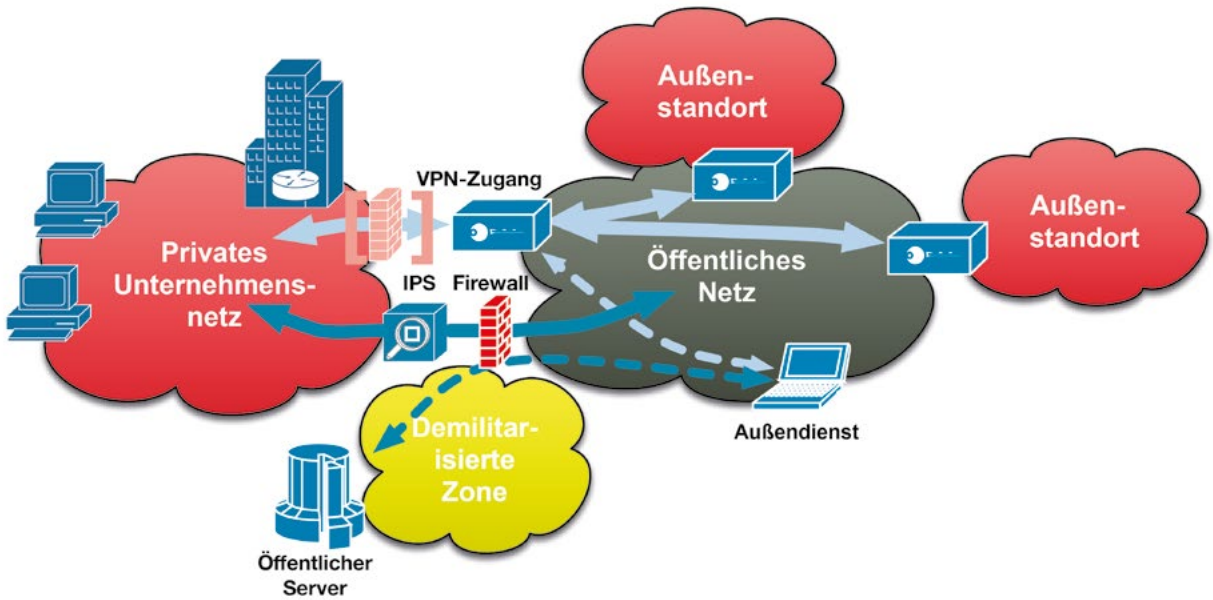


Abbildung 3: Mit App-Ray werden Android-Apps auf Sicherheitsmängel durchleuchtet.

## Sicherheit mobiler Geräte

Eine weitere Bedrohung für Unternehmensnetze entsteht durch verstärkte Nutzung von mobilen Endgeräten wie Smartphones und Tablets durch Mitarbeiter sowohl im privaten als auch im Unternehmensumfeld. Die Verwendung nur eines einzigen Gerätes für Arbeit und Freizeit ist nutzerfreundlich, birgt jedoch ein Risiko. Wenn die Geräte zu Hause mit den privaten Rechnern verbunden werden und somit Schadsoftware darauf gelangen kann, sind kritische Geschäftsdaten wie E-Mail oder Kontakte dem Zugriff Dritter ausgesetzt. Eine weitere Gefährdung stellen die zahlreichen Apps dar. Statistisch gesehen werden in Deutschland 54 Apps pro Sekunde heruntergeladen. Die Hälfte der Smartphone-Besitzer hat mehr als 50 Apps pro Smartphone im Einsatz. Den wenigsten ist bewusst, was die Apps im Hintergrund so alles tun. Das am AISEC entwickelte Analyse-Framework App-Ray (vgl. www.app-ray.de) ermöglicht eine vollautomatische Analyse und Einschätzung der Sicherheit von Android-Apps nach vorher vom Unternehmen selbst festgelegten Kriterien. Die Analyse der Apps ist flexibel und lässt sich an unterschiedlichste Firmen-Policies anpassen. Am AISEC wurde zudem ein „Trusted-App-Market“-Konzept entwickelt, das es Firmen erlaubt, eigene App Stores zu betreiben, die nur sichere Anwendungen zulassen. App-Ray kann als eigenständiges Tool, z.B. zum direkten Überprüfen von Smartphones, verwendet werden oder als Sicherheitsfeature in Enterprise App Stores und Mobile-Device-Management-Lösungen integriert werden. Dabei kann App-Ray auch als Qualitätsprüfungs-Tool von Unternehmen eingesetzt werden, die eigene Apps von Drittanbietern erstellen lassen.

**PROF. DR. CLAUDIA ECKERT**
Leiterin des Fraunhofer-Instituts für Angewandte und Integrierte Sicherheit, München
claudia.eckert@aisec.fraunhofer.de




SICHERUNGSMÖGLICHKEITEN

# Netzwerke schützen – aber wie?

*Die jüngsten Abhörskandale haben die Sicherheitsmängel im Bereich der IT offenkundig werden lassen. Wie lassen sich Angriffe und unerwünschte Zugriffe abwehren und gleichzeitig eine ausreichende Akzeptanz bei den Nutzern erreichen? Ein Überblick über technische Schutzmöglichkeiten und ihre Schwierigkeiten.*

Nicht zuletzt durch das Bekanntwerden der umfassenden Abhörtätigkeiten amerikanischer und britischer Geheimdienste ist der Bedarf für sichere Kommunikation erneut in das öffentliche Bewusstsein gerückt worden. Hierbei sind neben dem viel diskutierten Schutz der Privatsphäre der Bürger auch vertrauliche Informationen von Unternehmen und Behörden zu schützen. Denn gerade für eine moderne Wissensgesellschaft ist ein angemessener Schutz übertragener und verarbeiteter Informationen auch aus ökonomischen Gründen von zentraler Wichtigkeit.

Der Abhörskandal selbst kam für einige sicher nicht völlig unerwartet, da das in den 1970er-Jahren entwickelte Internet-Protokoll (IP) Daten im Klartext überträgt und keine signifikanten Schutzmechanismen bietet. Im Wesentlichen ist der Skandal somit Bestätigung lange gehegter Vermutungen und auch die prinzipiellen Gegenmaßnahmen sind bereits gut erforscht.

Primär sind dafür die übertragenen Daten mithilfe kryptographischer Algorithmen und Protokolle vor unberechtigter Einsichtnahme („Vertraulichkeit“) sowie möglicher Veränderungen durch Unberechtigte („Integrität und Authentizität“) zu schützen, bevor sie in Bereiche gelangen, die nicht unter der Kontrolle des Nutzers stehen.

Hierfür kann einerseits ein Schutz auf Anwendungsebene durch Protokolle wie Transport Layer Security (TLS) etwa unter Nutzung des anerkannten Advanced Encryption Standard (AES) implementiert werden. Im geschäftlichen Umfeld wird häufig zusätzlich bei der Übertragung von Daten über nichtvertrauenswürdige Netze für alle Anwendungen bereits auf der Ebene des Netzwerks eine Verschlüsselung erzwungen, indem sogenannte Virtuelle Private Netzwerke (VPN) aufgebaut werden.

Aber auch wenn die prinzipiellen Sicherungsmöglichkeiten bekannt sind, erfordert ihr richtiger Einsatz seit jeher ein relativ tiefes Verständnis für die eingesetzten Verfahren, Protokolle und Implementierungen. Dafür existieren mannigfaltige Gründe. So haben sich in der Vergangenheit als vertrauenswürdig vorauszusetzende Zertifizierungsinstanzen, die digitale Zertifikate über die Identitäten von Kommunikationspartnern ausstellen, wiederholt als unzuverlässig und unsicher erwiesen. Insbesondere der aktuelle Ansatz mit vielen unabhängigen Instanzen hat in der Vergangenheit immer wieder zu Problemen geführt, da das Kompromittieren einer einzigen dieser Instanzen zu einem vollständigen Verlust der Sicherheitseigenschaften führt, wie etwa die Comodo- und Digi-Notar-Hacks im Jahr 2011 gezeigt haben [Lea11]. Somit obliegt die Aufgabe der Identitätsprüfung oft dem Endnutzer, der diese in den meisten Fällen nicht mit ausreichender Verlässlichkeit erbringen kann.

Aufgrund der gegenüber Sicherungsmaßnahmen auf der Netzwerk-

ebene erhöhten Komplexität sind bei der anwendungsbasierten Verschlüsselung in den letzten Jahren eine ganze Reihe von Protokollschwächen und Implementierungsprobleme zutage getreten. Details zu einigen TLS-Schwächen finden sich etwa in [AP13, GHP13, Zol11].

Beim Einsatz kryptographischer Protokolle muss darüber hinaus zugesichert werden können, dass sämtlicher Verkehr nur über die entsprechenden Schnittstellen ausgetauscht werden kann und nicht etwa ein Dienst von der Sicherheitspolitik unberücksichtigt bleibt. In Unternehmen und Behörden wird dies in der Regel durch zentrale Firewalls erreicht, die unerwünschten Verkehr filtern.

Aber selbst wenn Sicherungsverfahren eingesetzt werden, sind oft keine sehr aussagefähigen Benchmarks der erreichten Sicherheitsziele möglich. Somit obliegt die Auswahl des richtigen Standards, Protokolls oder Produktes Experten, da eine objektive Bewertung der IT-Sicherheit immer voraussetzt, dass die Interna des Gesamtsystems und die Möglichkeiten der Angreifer vollständig verstanden werden.

Bei der Diskussion um die offensichtlichen Probleme, die der Abhörskandal zutage gefördert hat, nämlich denen bei der Sicherung von Vertraulichkeit, Integrität und Authentizität, tritt jedoch ein für unsere Wissensgesellschaft ebenso wichtiges Sicherheitsziel in den Hintergrund: die Verfügbarkeit der Informations- und Kommunikationsinfrastruktur selbst sowie der von ihr realisierten Dienste. Neben herkömmlichen Verfügbarkeitsmaßnahmen, wie sie etwa auch beim Stromnetz zum Einsatz kommen, existiert bei heutigen Kommunikationsnetzen eine weitere Anforderung: Denn selbst bei vorsätzlichen Sabotageangriffen von entfernten Rechnern – die in diesem Kontext oft als Denial-of-Service-Angriffe (DoS-Angriffe) bezeichnet werden – sollten Systeme und Dienste weiterhin korrekt und sicher funktionieren.

Im aktuellen „NSA-Skandal“ haben DoS-Angriffe zwar noch keine Rolle gespielt, doch haben die Konflikte zwischen Russland und Estland 2007 [Les07] sowie der Kaukasuskrieg 2008 [KK08] gezeigt, dass DoS-Angriffe auf Kommunikationsinfrastrukturen aufgrund politischer Spannungen durchaus zu beachtende Szenarien darstellen.

Gefährlich werden diese Angriffe wegen ihrer einfachen Durchführbarkeit. So ist etwa eines der Grundprinzipien des paketvermittelnden Internets die Zustellung von Datenpaketen, ohne dass der Empfänger sein Einverständnis gegeben haben muss (anders als bei leitungsvermittelnden Diensten, bei denen ein Verbindungsaufbauwunsch abgelehnt werden kann). Daher werden DoS-Angriffe häufig einfach durch das Senden großer Datenmengen unter Beteiligung einer Vielzahl zuvor kompromittierter Systeme von ansonsten unbeteiligten Nutzern ausgeführt. Solche Verbünde aus kompromittierten Systemen – sogenannte Bot-Netze – können auf dem digitalen Schwarzmarkt sogar stunden- oder tageweise für relativ geringe Beträge gemietet werden.

Ein wirkungsvoller Schutz gegen bandbreitenerschöpfende DoS-Angriffe ist nur beschränkt möglich. Im Wesentlichen können gefährdete Systeme zum einen redundant bzw. überdimensioniert ausgelegt werden, und zum anderen kann der entsprechende Verkehr beim Internet-Provider gefiltert werden. Leider sind beide Methoden konträr zu anderen Sicherheitsdiensten. So sind Firewalls und verschlüsselnde Komponenten heute zentrale Punkte in den Netzinfrastrukturen, über die sämtlicher Verkehr zur Durchsetzung der Sicherheitspolitik geleitet werden muss, und somit oft sehr anfällig für DoS-Angriffe. Werden die ausgetauschten Daten zusätzlich verschlüsselt, wird das Filtern von Verkehr beim Provider ebenfalls erheblich erschwert, da der Angreifer einfach beliebige Pakete erzeugen kann, welche die gleiche Struktur wie verschlüsselte Pakete haben, und nur im überlasteten Endgerät durch Entschlüsseln von korrekten Paketen unterschieden werden können.

Die Diskrepanz zwischen Benutzbarkeit, Verfügbarkeit und den „klassischen“ Sicherheitszielen verdeutlicht sich etwa bei den in Abbildung 1 illustrierten, etablierten Verfahren zur automatisierten VPN-Konfiguration [RS11], die häufig darauf beruhen, dass

- sie entweder alle Standorte über Tunnel mit einigen wenigen ausgezeichneten VPN-Gateways („Konzentratoren“) verbinden, wobei die Daten in den Konzentratoren umverschlüsselt werden
- oder sie VPN-weit für alle teilnehmenden VPN-Knoten bekannte Gruppenschlüssel verwenden, sodass für alle kryptographischen Tunnel der gleiche Schlüssel verwendet wird und bereits ein einziger kompromittierter VPN-Knoten dazu führen würde, dass alle Tunnel für den Angreifer „gläsern“ werden und die Daten nicht mehr schützen
- oder sie in allen VPN-Gateways Konfigurationsdaten für jeweils alle anderen möglichen Partnersysteme einrichten („Vollvermaschung“), was bei der Verbindung von $n$ Teilnehmern $n \times (n\text{-}1)/2$ Tunnel benötigt. Bei 500 Systemen wären dies also bereits 124.750 Tunnel.

Während manuell eingerichtete vollvermaschte VPN nicht nur einen hohen Arbeitsaufwand mit sich bringen, sondern auch anfällig für Konfigurationsfehler und unflexibel bei der Einbindung mobiler Teilnehmer sind, stellt die Verwendung von Konzentratoren einen potenziellen Leistungsengpass und, wie bereits angedeutet, auch ein erhebliches Verfügbarkeitsrisiko dar.

Lösungen, die auf VPN-weiten Gruppenschlüsseln beruhen, weisen erhebliche Sicherheitsdefizite auf, wie bereits durch Kompromittieren von Knoten eines konkreten VPN-Produkts praktisch nachgewiesen wurde [RS09]. Weiterhin sollte auch die Abhängigkeit von zentralen „Leit- bzw. Planungsstellen“ – z. B. in Form von zentralen Schlüsselverteilungsservern etc. – vermieden werden, da sonst im Falle eines Ausfalles dieser zentralen Stellen das VPN anfällig für Sabotageangriffe wird.

Um diese Nachteile zu umgehen, wurde unter anderem das Secure OverLay for IPsec Discovery (SOLID) entwickelt [RSS10], welches konsequent auf den Einsatz von Peer-to-Peer-Technologien setzt. Es verteilt so die Verwaltungsaufgaben auf alle jeweils gleichberechtigt agierenden VPN-Gateways und erreicht so

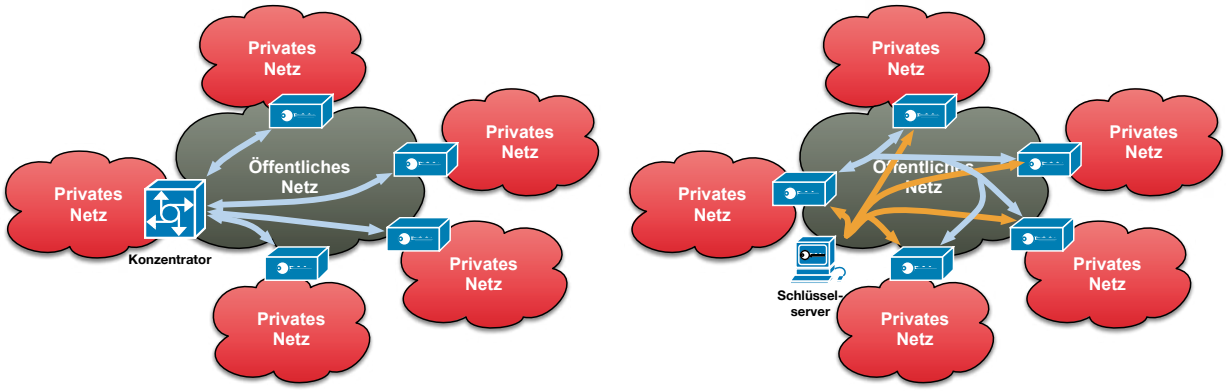



Abbildung 1: Typische VPN-Szenarien: Im Bild links gibt es einen zentralen Konzentrator. Im mittleren Bild ist ein Gruppenschlüssel-basiertes Verfahren skizziert,

bei minimalem Konfigurationsaufwand nicht nur eine hohe Leistungsfähigkeit und Skalierbarkeit, sondern auch eine hohe Ausfallsicherheit, da die Funktionsfähigkeit eines mit SOLID eingerichteten VPN nicht mehr von einzelnen Systemen abhängt.

In SOLID kommt dabei eine logische Ringstruktur zum Einsatz, die durch sichere Tunnel über der vorhandenen Transportinfrastruktur errichtet wird. Somit können neu hinzukommende VPN-Gateways bereits durch den Aufbau von nur zwei Tunnel sehr schnell in das VPN integriert werden. Durch den anschließenden Aufbau von logarithmisch vielen Querverbindungen im Ring, ähnlich zu den etablierten P2P-Ansätzen Chord oder Pastry, verkürzt sich die Zeit zum Finden anderer Gateways. Weitere Verbindungen werden je nach Lastsituation im Netzwerk aufgebaut. Im Unterschied zu bestehenden Autokonfigurationsansätzen werden alle Nachrichten grundsätzlich in einem sogenannten inneren Ende-zu-Ende-Tunnel verschlüsselt übertragen und können bei Vermittlung über Zwischensysteme des VPN von diesem nicht vollständig entschlüsselt und damit mitgelesen werden.

Die Authentisierung der Teilnehmer erfolgt dabei durch Zertifikate, in denen unter anderem die IP-Adressbereiche attestiert werden. Somit können auch kompromittierte VPN-Knoten erstmals bei einer VPN-Autokonfiguration keine Pakete unbemerkt mit falschen Ursprungsadressen senden. Darüber hinaus werden durch Einbettung der logischen Ringstruktur in komplexere Transportnetze auch in mehrere Sicherheitszonen organisierte („verschachtelte“) Netzwerke und VPN-Knoten unterstützt, die von Network Address Translation betroffen sind, also sich in Netzbereichen befinden, in denen private IP-Adressen verwendet werden, welche im globalen Internet nicht gültig sind. Hierdurch kann erstmalig auch ein einfach beherrschbarer Betrieb von mehrstufig gesicherten Kommunikationsinfrastrukturen und damit ein nochmals höheres Sicherheitsniveau als mit herkömmlichen Lösungen realisiert werden.

## Implementierungsspezifische Fragestellungen

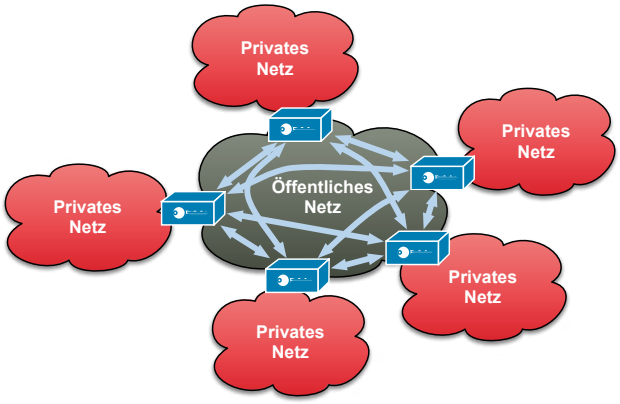
Zusätzlich zur Untersuchung konzeptioneller Fragestellungen befindet sich auch die Bewertung implementierungsspezifischer Fragestellungen in einem voll funktionsfähigen Prototyp zurzeit im Fokus der Forschung (siehe Abbildung 2). Der entwickelte Prototyp basiert auf Linux/strongSwan und wird in diese Umgebung durch eine Reihe komplexer Schnittstellen an eine unmodifizierte IPsec-Implementierung angebunden. Für die Evaluierung sehr großer VPN kann der gleiche Quellcode im Kontext einer Simulationsumgebung ausgeführt werden. Vergleichsmessungen haben gezeigt, dass Unterschiede zwischen Simulation und Realität auf diese Weise nur um etwa zehn Prozent abweichen.

Eine Herausforderung hierbei ist die Überwachung und die Verwaltung solcher verteilten Sicherheitsarchitekturen, die sich stark von herkömmlichen Verfahren unterscheiden. Wie werden etwa digitale Zertifikate auf eventuellen Rückruf geprüft, ohne auf zentrale Instanzen zuzugreifen? Heutige Monitoring-Verfahren, die unter anderem Angriffe beobachten könnten, gehen davon aus, dass die überwachten Komponenten immer unter bestimmten Adressen verfügbar sind; wie wird in flexibleren Netzen damit umgegangen, dass Knotenteilnahme und kryptographische Verbindungen fluktuieren?

## Ausblick auf zukünftige Verfahren

Zukünftige Verfahren zur Sicherung unserer Kommunikationsinfrastrukturen müssen sich somit bereits auf Netzwerkebene flexibel an den tatsächlichen Kommunikationsbedürfnissen der Nutzer orientieren, also beispielsweise individuelle VPN-Tunnel nach Bedarf einrichten. Gleichzeitig müssen exponierte Systeme vermieden werden, etwa indem Firewall-Regeln nicht an einem zentralen Ort, sondern „im Netz“ durchgesetzt werden. Nur so wird es möglich sein, neuen Sicherheitsbedrohungen angemessen zu begegnen und gleichzeitig eine ausreichende Akzeptanz bei den Nutzern zu erreichen.

Wenn neue Technologien dies ermöglichen, kann ein solcher Schutz auf der Ebene der Kommunikationsinfrastruktur gewährleisten, dass die Anwendungen aller Teilnehmer an diese Entscheidungen gebunden sind




die rechte Abbildung hingegen zeigt das Szenario einer Vollvermaschung.

und sie nicht etwa bestimmte Daten an einer kryptographischen Sicherung vorbeisenden können. Durch einen solchen einheitlichen Schutz könnte dann beispielsweise auch die Verwendung sicherer Verschlüsselungsalgorithmen einfacher erzwungen werden – eine Funktionalität, die selbst bei Anwendungen mit TLS-Unterstützung oft nicht implementiert ist. Darüber hinaus bieten die Endgeräte weniger Angriffsfläche, wenn eine kryptographische Authentisierung aller verarbeiteter Nachrichten erzwungen wird. Vor dem Hintergrund des NSA-Skandals wird ein weiterer potenzieller Vorteil der Verschlüsselung auf Netzwerkebene offenbar: Durch das Bündeln von Netzwerkpaketen unterschiedlicher Dienste und Klienten in einem kryptographisch gesicherten Tunnel, wäre eine Verkehrsflussanalyse (insbesondere in verschachtelten VPN-Konfigurationen) nur noch sehr eingeschränkt möglich. Eine einfache Forderung nach einer Ende-zu-Ende-Verschlüsselung auf Anwendungsebene als Reaktion auf die aktuellen Ereignisse scheint somit zu kurz zu greifen.

**PROF. DR.-ING. GÜNTER SCHÄFER UND DR.-ING. MICHAEL ROSSBERG**
Technische Universität Ilmenau,
Fachgebiet Telematik/Rechnernetze

## Literaturhinweise

[AP13] AlFardan, N, Paterson K.: Lucky thirteen: Breaking the TLS and DTLS record protocols. IEEE Symposium on Security and Privacy. 2013.
[GHP13] Gluck, Y., Harris, N., Prado A. Breach: Reviving the Crime Attack. 2013.
[KK08] Kastenberg, J.E., Korns, S.W.: Georgia's cyber left hook. Parameters 38.4, pp. 60–76, 2008.
[Lea11] Leavitt, N.: Internet Security under Attack: The Undermining of Digital Certificates. Computer, 44.12, pp. 17-20, 2011.
[Les07] Lesk, M.: The New FrontLine: Estonia under Cyberassault. Security & Privacy 5.4, pp. 76–79. 2007.
[RS09] M. Roßberg, G. Schaefer. Ciscos Group Encrypted Transport VPN – Eine kritische Analyse. D-A-CH Security 2009, Ruhr-Universität Bochum, Mai 2009.
[RSS10] Rossberg, M., Schaefer, G., Strufe, T.: Distributed Automatic Configuration of Complex IPsec-Infrastructures. Network and Systems Management, 18.3, pp. 300-326, 2010.
[RS11] Rossberg, M, Schaefer, G.: A survey on automatic configuration of virtual private networks. Computer Networks, 55.8, pp. 1684-1699, 2011.
[Zol11] Zoller, T.: TLS & SSLv3 renegotiation vulnerability, 2011.

Abbildung 2: Der mit dem GI/ITG/VDE Communication Software Award ausgezeichnete SOLID-Prototyp auf der Netsys 2013

E-MAIL-SICHERHEIT

# Kryptographie: Methoden und Metapher

*Ein Großteil des E-Mail-Verkehrs ist unerwünschten Einblicken bislang weitgehend schutzlos ausgeliefert. Kryptographische Verfahren können das Problem abhörsicherer Nachrichtenübertragung zwar nicht lösen, die Sicherheit vor allem bei richtiger Implementierung und Anwendung aber deutlich erhöhen.*

Auf die Berichte der letzten Monate über den Umfang, in dem Geheimdienste die Kommunikation von Privatpersonen, Firmen, und Politikern aufzeichnen, seien es Telefongespräche, E-Mails oder Zugriffe auf Webseiten, wird einerseits mit dem Hinweis geantwortet, dass geeignete kryptographische Schutzverfahren bereits existieren und es die Nachlässigkeit der Benutzer sei, diese nicht zu verwenden. Andererseits liest man, dass die NSA sichere, d.h. kryptographisch geschützte, Verbindungen zu Webseiten wie Facebook oder Google umfassend mitlesen würde.

Diesem scheinbaren Widerspruch soll nun am Beispiel von E-Mail nachgegangen werden. Eine neu eingetroffene E-Mail wird üblicherweise in Form eines Symbols angezeigt, das einen Briefumschlag darstellt. So wird suggeriert, dass die Nachricht während der Übertragung in diesem Umschlag verschlossen sei und man ihn erst öffnen müsse, um den Inhalt der E-Mail sehen zu können. Dieser Vergleich hinkt. Den Tatsachen näher kommt ein Blatt Papier mit Senderadresse (nicht notwendigerweise der Wahrheit entsprechend), Empfängeradresse und dem Text der Nachricht. Dieses Memo ist für alle an der Übermittlung Beteiligten lesbar.

## Symmetrische Verschlüsselung

Der Vergleich mit dem Postwesen hinkt auch am zweiten Fuß. Bei einem Brief kann nachverfolgt werden, wo er sich gerade befindet, und er befindet sich immer an genau einer Stelle. E-Mail ist ein verteiltes Dateiverwaltungssystem. Eine E-Mail wird von Rechner zu Rechner weiterkopiert. Teile einer E-Mail können sich während der Zustellung gleichzeitig an verschiedenen Orten befinden, und selbst nach der Zustellung können Kopien der E-Mail an den beteiligten Rechnern eine gewisse Zeit lang weiterbestehen (siehe Abbildung 1).

Wie kann nun eine Nachricht in den metaphorischen Umschlag gesteckt werden, sodass sie während der Zustellung nicht gelesen werden kann? Man verschlüsselt sie. Man versperrt nun kaum Briefumschläge mit einem Schlüssel und so greifen wir auf die Metapher einer verschließbaren Kassette zurück. Der gleiche Schlüssel wird zum Verschlüsseln (sperren) und Entschlüsseln (öffnen) verwendet; man spricht von symmetrischer Verschlüsselung. Sind Sender und Empfänger an verschiedenen Orten, braucht man zwei Exemplare des Schlüssels. Das wirft die Frage auf, wie Sender und Empfänger dazu kamen, gleiche Schlüssel zu besitzen. Dies ist die Crux der Kryptographie: Sie löst Probleme der sicheren Nachrichtenübertragung nicht; sie verwandelt sie in Probleme der Schlüsselverwaltung.

Das vorliegende Schlüsselverwaltungsproblem kann gelöst werden, indem man seinem Partner eine Kopie des Schlüssels persönlich übergibt. Das ist dann plausibel, wenn persönliche Kontakte in der physischen Welt mit vertretbarem Aufwand arrangiert werden können. Eine Terroristenzelle könnte so, nach einem klandestinen Treffen, ihre verschwörerischen Nachrichten sicher versenden.

## Public-Key-Verschlüsselung

Public-Key-Kryptographie vermeidet, geheime Schlüssel austauschen zu müssen: „Der Sender verschlüsselt die Nachricht mit dem öffentlichen Schlüssel des Empfängers, der sie mit seinem privaten Schlüssel entschlüsselt“. Als Metapher aus dem Briefverkehr diene ein sicherer Briefkasten, der außen durch eine Zahlenfolge (dem öffentlichen Schlüssel, kein Schlüssel zum Sperren, sondern ein Schlüssel zum Suchen, wie in einer Datenbank) gekennzeichnet ist. Jeder kann Briefe einwerfen (mit der kryptischen Zahlenfolge verschlüsseln), sofern die Existenz des Briefkastens bekannt ist. Eingeworfene Briefe können nur entnommen werden, indem der Briefkasten mit dem privaten Schlüssel, der nur in einem Exemplar existieren muss, aufgesperrt wird (Entschlüsseln der Nachricht). Wie oben angedeutet existiert dieser metaphorische Briefkasten gleichzeitig beim Sender und Empfänger (siehe Abbildung 2).

Hat ein Empfänger einen Briefkasten wie in Abbildung 2, kann man ihm direkt sichere Nachrichten zukommen lassen. Hat nur sein E-Mail-Anbieter einen öffentlichen und privaten Schlüssel, kann man Nachrichten in den Sammelbriefkasten des Anbieters einwerfen. Dritte sehen den Inhalt der Nachrichten nicht, der Anbieter sehr wohl.

## Digitale Signaturen

Mit kryptischen Zahlen markierte Briefkästen sind nicht gerade benutzerfreundlich. Lieber fände man auch den Namen des Empfängers auf dem Briefkasten. Namen auf Briefkästen zu schreiben, sei es den eigenen oder einen fremden, ist kein Problem. Das neue Schlüsselverwaltungsproblem ist, sicherzustellen, dass der, dessen Namen mit am Briefkasten steht, tatsächlich den zugehörigen privaten Schlüssel besitzt. Ansonsten

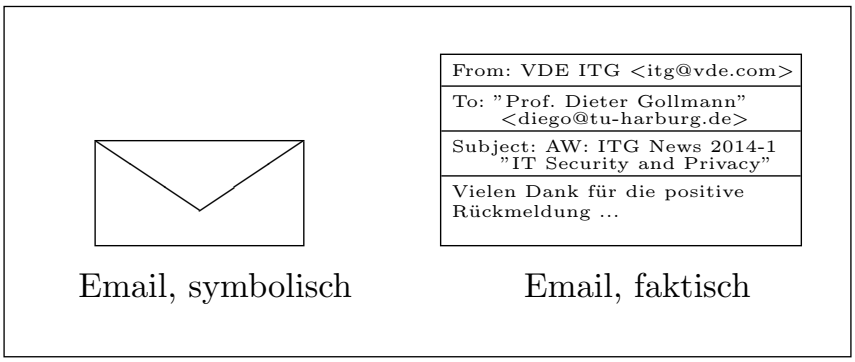



Abbildung 1: E-Mails werden oft durch einen geschlossenenn Briefumschlag symbolisiert. Faktisch ist eine E-Mail eine offene Nachricht inklusive Angaben über Sender und Empfänger.

würde ja ein anderer den Briefkasten öffnen und die Nachrichten lesen können. Das neue Problem könnte wie folgt gelöst werden:

- Persönliches Treffen, bei dem der Empfänger seine kryptische Briefkastennummer übergibt. Der Sender merkt sich Namen und Briefkastennummer.
- Der Empfänger teilt seinen öffentlichen Schlüssel auf ungesicherte Weise mit, etwa per E-Mail. Außerdem publiziert er auf anderem Wege, z. B. auf seiner Webseite, einen Fingerabdruck dieses Schlüssels, berechnet mit einer kryptographischen Hashfunktion (Einwegfunktion). Ein Sender kann so prüfen, ob der veröffentlichte Fingerabdruck mit dem des erhaltenen Schlüssels übereinstimmt. Diese Methode benötigt keine dritte Partei und verlässt sich darauf, dass ein Angreifer nicht gleichzeitig E-Mail und Webseite fälschen kann.
- Am Briefkasten steht nur der Name, d. h. der Name ist der öffentliche Schlüssel (Identitätsbasierte Kryptographie). Der private Schlüssel wird aus dem Namen abgeleitet. Dazu bedarf es eines Dienstanbieters, dem vertraut wird, diese Ableitung korrekt durchzuführen und den privaten Schlüssel nicht auch selbst zu verwenden. In unserer Metapher könnte man sich als Dienstanbieter die Post vorstellen, die sichere Briefkästen mit (privatem) Schlüssel liefert, und der man vertraut, keine Zweitschlüssel anzufertigen.
- Ein Dienstanbieter (Zertifizierungsstelle) bestätigt die Zuordnung der kryptischen Briefkastennummer an einen Namen. Den privaten Schlüssel bekommt der Dienstanbieter nicht notwendigerweise zu Gesicht.

Den vierten Fall findet man in der Praxis am häufigsten. Er löst aber unser Schlüsselverwaltungsproblem nicht. Er wandelt es weiter. Wie kann der Sender einer ihm vorgelegten Zuordnung trauen? Dazu verwendet man digitale Signaturen. Die Zertifizierungsstelle signiert mit ihrem privaten Unterschriftsschlüssel; überprüft wird mit dem zugehörigen öffentlichen Verifikationsschlüssel. Die Metapher des Unterschreibens hat ihre Tücken. Unterschrift suggeriert, dass dem Unterschriebenen vertraut werden kann. Das ist nicht notwendigerweise der Fall. Eine digitale Signatur besagt nicht, dass der Inhalt eines Dokuments wahr ist. Eine digitale Signatur besagt nicht, wer das Dokument unterschrieben hat. Eine digitale Signatur ordnet das signierte Dokument dem öffentlichen Schlüssel zu. Dazu passt das Bild eines versperrbaren, nummerierten, gläsernen Aktenschranks. Jeder sieht, was darin abgelegt ist. Nur der Besitzer des privaten Schlüssels kann Dokumente ablegen. Wer der Besitzer ist, sieht man nicht; am Schrank steht wieder eine kryptische Zahlenfolge (der öffentliche Schlüssel).

## Zertifikate

Zertifikate sind signierte Dokumente, die öffentlichen Schlüsseln Namen zuordnen. Eine beliebte Metapher ist ein Lichtbildausweis, der ein Bild einem Namen zuordnet. Die Gefahr bei dieser Metapher ist, dass sie dazu verleitet, Zertifikate generell als amtliche Dokumente zu betrachten, ausgestellt von vertrauenswürdigen Behörden. Dies ist in der Realität des Internets ganz und gar nicht der Fall. Andererseits ist diese Metapher für unsere Zwecke doch nicht so schlecht, denn Behörden können ihre eigenen Agenten durchaus mit falschen Papieren ausstatten.

Zertifikate sind also die Dokumente im gläsernen Aktenschrank einer Zertifizierungsstelle. Das können Dokumente sein, die Namen und öffentliche Verschlüsselungsschlüssel von Nutzern angeben (Endnutzerzertifikate). Ein Dokument im Aktenschrank könnte dessen Besitzer angeben (selbstsigniertes Zertifikat). Information über den Besitzer könnte als Ausstellerzertifikat auch in einem anderen Aktenschrank abgelegt sein. Dann ist dessen Besitzer zu eruieren, und so weiter und so fort. Am Ende steht der Sender vor einem gläsernen Aktenschrank und vertraut auf Gedeih und Verderb der Information, die er dort findet. In der Sprache der Kryptographie ist diese Endstation ein „vertrauenswürdiges[1] Wurzelzertifikat". Wenn von einer Public Key Infrastructure die Rede ist, so steht im Kern so ein Geflecht von Zertifizierungsstellen dahinter, das dazu dient, kryptische Zahlenfolgen ihren tatsächlichen Besitzern zuzuordnen.

## Transport Layer Security (TLS)

Der Zugriff auf „sichere" Webseiten wird über das TLS-Protokoll (früher SSL) abgewickelt. Mit diesem Protokoll kommen ein Client und ein Server, die anfangs nichts voneinander wissen, zu einem gemeinsamen Geheimnis. Der Server teilt seinen öffentlichen Schlüssel in einem Zertifikat mit. Der Client überprüft dieses Zertifikat, wozu er das Wurzelzertifikat des Ausstellers benötigt, erzeugt ein neues Geheimnis und versendet es verschlüsselt mit dem öffentlichen Schlüssel des Servers. Der Server entschlüsselt das Geheimnis mit seinem privaten Schlüssel. Weitere Nachrichten werden aus Effizienzgründen symmetrisch verschlüsselt. In unserem Bild deponiert der Client den Schlüssel für eine verschließbare Kassette im sicheren Briefkasten des Servers. Er vertraut der Zertifizierungsstelle, ihn zum richtigen Briefkasten zu weisen.

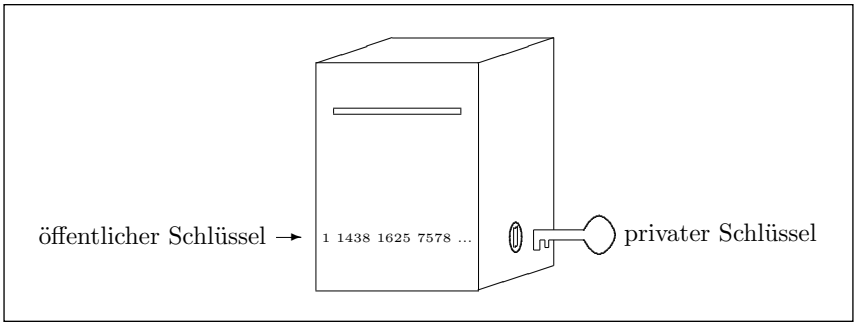



Abbildung 2: Das Prinzip der Public-Key-Verschlüsselung: der öffentliche Schlüssel bezeichnet den Briefkasten, der private Schlüssel öffnet ihn.

Wer die Liste der Wurzelzertifikate des Senders kontrolliert, kontrolliert wem der Sender bei der Zuordnung von öffentlichen Schlüsseln an Namen vertraut. Heute wird diese Liste mit dem Webbrowser (Google, Microsoft, …) oder dem Gerät (Apple) mitgeliefert. Diesen Quellen wird (fast) blind vertraut. Nachrichtendienste könnten den kryptographischen Schutz hier an seiner Wurzel aushebeln und ihnen genehme Zertifizierungsstellen eintragen lassen. Auf Seite des Empfängers ist der private Schlüssel zu schützen. Dies ist selbst für professionelle Systembetreiber keine einfache Aufgabe. Man muss davon ausgehen, dass hier verbreitet Schwachstellen bestehen.

## Sicherheit der kryptographischen Verfahren

Der Dritte im Bunde ist die Zertifizierungsstelle. Zertifizierungsstellen unterliegen keiner Beschränkung, für wen Zertifikate ausgestellt werden dürfen. Das ist eine generelle Schwäche. Bei Kompromittierung einer beliebigen Zertifizierungsstelle ist so niemand mehr sicher. Der Angreifer kann gezielt falsche Endnutzer- oder Ausstellerzertifikate erzeugen, ohne dass die angegebenen Besitzer der Zertifikate davon Kenntnis haben. Bei einem Angriff auf die niederländische Zertifizierungsstelle DigiNotar wurden etwa falsche Zertifikate für Google ausgestellt, mit denen der Angreifer „sichere“ Google-Anwendungen vortäuschen konnte. Dieser Vorfall führte dazu, dass DigiNotar den Betrieb einstellen musste. In einem anderen Fall wurde versehentlich ein Ausstellerzertifikat statt eines Endnutzerzertifikats ausgestellt. Damit war eine neue Zertifizierungsstelle geschaffen, die nun falsche Zertifikate ausstellen konnte, die bei der Überprüfung als vertrauenswürdig eingestuft wurden.

In unseren Metaphern sind die kryptographischen Verfahren das Material, aus dem die Kassetten, sicheren Briefkästen und gläsernen Aktenschränke konstruiert sind. Diese Verfahren mögen nicht beweisbar sicher – sozusagen nicht garantiert unbrechbar – sein, aber sie bieten im Vergleich zu den Schlüsselverwaltungslösungen ein wesentlich höheres Sicherheitsniveau. Für symmetrische Verschlüsselung gibt es z. B. AES (US-Standard, nach öffentlicher Kandidatensuche wurde ein Verfahren belgischer Kryptographen gewählt), für kryptographische Hashfunktionen SHA-3 (US-Standard, nach öffentlicher Kandidatensuche wurde ein Verfahren europäischer Kryptographen gewählt). Diese Verfahren werden als sicher angesehen, weil eine intensive Analyse in der öffentlichen Forschung keine wirklichen Schwachstellen aufdecken konnte. Sie haben also die geläufigen Belastungstests unbeschadet überstanden.

Die heute in der Praxis eingesetzten Public-Key-Verfahren beruhen auf der Schwierigkeit zahlentheoretischer Probleme, etwa der Zerlegung des Produkts zweier großer Primzahlen in seine Faktoren. Die Aussagen zur Schwierigkeit sind aber empirische Feststellungen, nicht bewiesene Fakten. Die beweisbar sicheren Konstrukte der kryptographischen Forschung sind so oft imposante Gebäude, gegründet auf dem Sand unbewiesener Annahmen. Empfehlungen zur Algorithmen- und Parameterwahl vom Bundesamt für Sicherheit in der Informationstechnik haben daher einen typischen Horizont von sechs Jahren.[2]

Gelegentlich gelangen Meldungen über gebrochene kryptographische Verfahren bis in die Massenmedien. Die vorherigen Bemerkungen könnten den Verdacht erwecken, dass sich da das lose Fundament verschoben und grundsätzliche Lücken offengelegt hätte. Dem ist aber meist nicht so. Die Ursachen sind eher handwerkliche Schwächen in Implementierungen oder in technischen Details von Standards, sei es

- im Zusammenspiel von kryptographischen Algorithmen und dem Padding von Nachrichten[3, 4],
- dass der Zeitpunkt von Fehlermeldungen Information über den aktuellen Bearbeitungsschritt und weiter über den Inhalt einer Nachricht preisgibt,
- dass auf einer höheren Protokollebene inkorrekte Annahmen über die Sicherheitsgarantien eines Protokolls auf einer tieferen Ebene gemacht werden[5],
- dass zwei gleichzeitig auf verschiedenen Protokollebenen konstruierte sichere Verbindungen nicht über deren Endpunkte einig sind.

## Man-in-the-Middle-Angriffe

Abbildung 3 skizziert eine Situation, in der sich ein E-Banking-Kunde mittels TLS mit seiner Bank verbinden wollte, aber unbemerkt beim Angreifer gelandet war. Wie üblich war TLS so benutzt worden, dass der Server authentifiziert wird, der Nutzer aber anonym bleibt. Der Kunde hätte die Verbindung zum Angreifer aus Unachtsamkeit akzeptieren können, etwa weil dessen Namen dem des Bank-Servers ähnelt. Der Angreifer hätte sich selbst im Browser des Kunden in die Liste der Wurzelzertifikate eintragen (lassen) können und ein falsches Zertifikat für den Bank-Server ausstellen können. Dieses Zertifikat wäre dann vom Browser anstandslos akzeptiert worden. Der Angreifer hätte in eine Zertifizierungsstelle einbrechen und sich dort ein Zertifikat für den Bank-Server oder ein Ausstellerzertifikat erzeugen können; die Zertifizierungsstelle hätte mit Hinweis auf Sicherheitsgesetze angehalten wer-

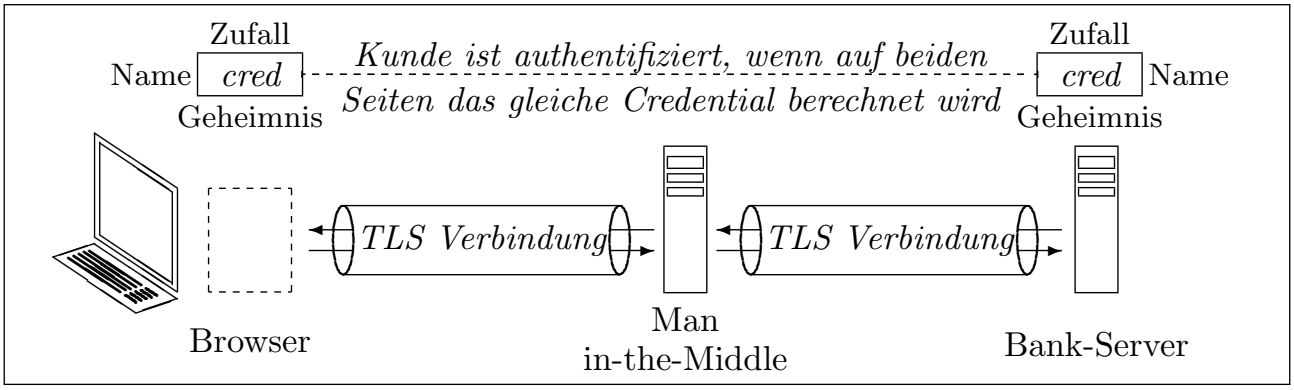



Abbildung 3: In diesem Szenario landet ein E-Banking-Kunde, der sich mittels TLS mit seiner Bank verbinden wollte, unbemerkt beim Angreifer. Ein Man-in-the-Middle-Angriff trotz sicherer Verbindungen.

den können, so ein Zertifikat auszustellen. Wie dem auch sei, der Angreifer baut nun seinerseits eine TLS-Verbindung zum Server auf.

Der Browser des Kunden öffnet nun in seiner sicheren Verbindung eine Webseite, auf der sich der Kunde mit Benutzername und Passwort beim Bank-Server anmeldet. Wenn Kunde und Server ein gemeinsames Geheimnis besitzen, so könnte der Kunde mit folgendem Verfahren authentifiziert werden, das man in verschiedenen Nuancen im Web (HTTP Digest Authentication) und im Mobiltelefonbereich (GSM/UMTS Subscriber Authentication) findet. Der Kunde teilt dem Server seinen (angeblichen) Namen mit. Der Server antwortet mit einer Zufallszahl. Der Browser berechnet aus Benutzernamen, Geheimnis, Zufallszahl und vielleicht noch weiteren relevanten Parametern ein Credential, das er dem Server schickt. Der Server führt mit seiner Version der Eingaben die gleiche Berechnung wie der Browser durch und vergleicht das eigene Resultat mit dem erhaltenen. Stimmen die Werte überein, ist der Kunde authentifiziert.

## Quantenkryptographie

Während sich der Kunde anmeldet, reicht der Angreifer die Nachrichten zwischen Browser und Server unverändert weiter. Weist sich der Kunde erfolgreich aus, schließt der Server fälschlich, dass er eine TLS-Verbindung zum Kunden hat. Die Präsenz des Angreifers kann entdeckt werden, wenn das Credential auch von Parametern der TLS-Verbindung abhängt[6] (siehe Abbildung 2). Seit dem Verfahren von Shor zum Faktorisieren auf Quantencomputern ist sich die kryptographische Forschung bewusst, dass ihr wichtige Fundamente wegbrechen können. Forschung zu Post-Quantum-Kryptographie sucht nach Verfahren, die alternative mathematische Grundlagen haben. Quantenkryptographie verspricht, sichere Nachrichtenübertragung auf die Gesetze der Quantenphysik rückführbar zu machen.[7] Theoretisch mag dies zutreffen. Praktisch kann es der Fall sein, dass die reale Implementierung eines theoretisch sicheren Verfahrens doch technische Lücken hat.[8, 9, 10] Zudem folgt aus der sicheren Übertragung nicht, dass man weiß, wer die Daten am anderen Ende in Empfang nimmt. Wie bei der klassischen Kryptographie steht man vor der Aufgabe, den Endpunkt einer Verbindung zu authentifizieren. Quantenkryptographie ist somit eine Lösung für diejenigen, die Antworten auf die schwierigen Fragen gefunden haben und sicher sein können, mit bekannten, sicheren Endpunkten verbunden zu sein. Das mögen vielleicht Firmen oder Behörden sein, die den Datenverkehr zwischen verschiedenen festen Standorten sichern wollen.

## Fazit

Kryptographie löst das Problem der abhörsicheren Nachrichtenübertragung nicht, sie ist aber trotzdem unverzichtbar. Praktische Probleme in der Schlüsselverwaltung treten dort auf, wo man anderen (Zertifizierungsstellen und Softwareentwicklern) und sich selbst (nolens volens sind wir für die sichere Konfiguration unserer Endgeräte verantwortlich) vertrauen muss. Vertrauen ist schlecht für Sicherheit. Das wussten schon die Römer und Lenin. Gerade wurde durch die NSA daran erinnert.

**DIETER GOLLMANN**
Institut für Sicherheit in verteilten Anwendungen
TU Hamburg-Harburg

## Fußnoten

[1] Information, der man auf Gedeih und Verderb vertrauen muss, als vertrauenswürdig zu bezeichnen, ist mehr als fragwürdig.

[2] BSI TR-02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version: 2013.02, 9.1.2013

[3] Daniel Bleichenbacher: Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1}, 1998

[4] Nadhem J. AlFardan and Kenneth G. Paterson: Lucky Thirteen: Breaking the TLS and DTLS Record Protocols, 2013

[5] Marsh Ray, Steve Dispensa: Renegotiating TLS, November 2009

[6] Rolf Oppliger, Ralf Hauser, David Basin: SSL/TLS Session-Aware User Authentication Revisited, Computers & Security, 2008

[7] FAZ: Quantenverschlüsselung: Den NSA Lauschern keine Chance, 27.10.2013

[8] IEEE Spectrum: Quantum Cryptography Cracked: Swedes find vulnerability in supposedly secure quantum cryptography system, 29.4.2008

[9] Phys. Rev. A: Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, 2008

[10] Nature Photonics: Hacking commercial quantum cryptography systems by tailored bright lumination, 2010

GRUNDRECHTE UND DATENSCHUTZ

# Persönlichkeitsschutz in einer vernetzten Welt

*Unternehmen und Geheimdienste gefährden so zentrale Grundrechte wie informationelle Selbstbestimmung und Telekommunikationsgeheimnis. Um die Bürger zu schützen, braucht es eine Allianz von Recht und Technik – also auch Infrastrukturen, die es ermöglichen, auf Gefährdungen automatisch zu reagieren.*

Der Schutz der Persönlichkeit gerät immer stärker unter Druck. Staaten und Unternehmen ignorieren ihn in einem bisher nicht vorstellbaren Umfang. Als normatives Gegenmodell gewinnen die Grundrechte der informationellen Selbstbestimmung und des Telekommunikationsgeheimnisses daher zunehmend an Bedeutung. Sie zu gewährleisten, wird jedoch immer schwieriger und erfordert neue Formen des Schutzes. In diesem Beitrag wird erläutert, warum die Grundrechte wichtig sind, worin ihre aktuelle Gefährdung besteht, wie sie vom geltenden Recht geschützt werden, warum dieser Schutz unzureichend ist und wie Ansätze zu einem verbesserten Schutz beschaffen sein müssen.

## Selbstbestimmung und Telekommunikationsgeheimnis

Die Rechtsordnungen in Europa und in Deutschland schützen übereinstimmend Grundrechte und Demokratie gegen Gefährdungen durch die automatisierte Datenverarbeitung. Artikel 7 und 8 der europäischen Grundrechtecharta, Artikel 8 der europäischen Menschenrechtskonvention und Artikel 1, 2 und 10 Grundgesetz (GG) sichern Menschenwürde und Freiheit durch den Daten- und den Geheimnisschutz. Das Bundesverfassungsgericht (BVerfG) hat aus diesen verfassungsrechtlichen Vorgaben risikogerecht das Grundrecht auf „informationelle Selbstbestimmung“ abgeleitet. Dieses gibt dem Betroffenen die Befugnis, „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“ (BVerfGE 65, 1 (43)). Die informationelle Selbstbestimmung hat eine subjektive und eine objektive Schutzrichtung.

Als subjektives Recht ist sie Voraussetzung für die Entscheidungsfreiheit in jedem Einzelfall. Kann der Betroffene nicht selbst über die ihn betreffenden Angaben entscheiden und daher nicht wissen, was andere über ihn wissen, kann er „in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden“ (BVerfGE 65, 1, 43). Die Selbstbestimmung ist aber auch Voraussetzung für die freie Entwicklung und Entfaltung der Persönlichkeit jedes Einzelnen. Damit ist die informationelle Selbstbestimmung die Voraussetzung für die Wahrnehmung aller Grundrechte. Ohne selbstbestimmten Informationsaustausch ist jede Verwirklichung von Grundrechten durch Kommunikation gefährdet. Daher muss der Einzelne auch in einer vernetzten Welt in der Lage sein, selbst zu entscheiden, welche Daten er über sich in welcher Rolle und in welcher Kommunikation preisgibt. Diesen Vorrang autonomer Entscheidung über Informationsfreigaben schützt das Grundrecht auf informationelle Selbstbestimmung.

Als Vorgabe für die Ordnung der Gesellschaft ist informationelle Selbstbestimmung „eine elementare Funktionsbedingung“ der Demokratie (BVerfGE 65, 1 (43)). Demokratisches Engagement wird es nur geben, wenn es nicht registriert wird und die registrierten Daten nicht gegen den Betroffenen verwendet werden können. Dabei schützt das Grundrecht auch vor einem Einschüchterungseffekt, der durch heimliche Datenverarbeitung entstehen kann. Informationelle Selbstbestimmung und Telekommunikationsgeheimnis zielen somit auf eine Kommunikationsordnung, die einen selbstbestimmten Informationsaustausch und eine freie demokratische Willensbildung ermöglichen. In diese Grundrechte greift derjenige ein, der Daten des Betroffenen gegen seinen Willen verarbeitet – unabhängig davon, ob dies eine staatliche Behörde oder ein privates Unternehmen ist. Der Betroffene ist in beiden Fällen gleich schutzwürdig. Die Missachtung seiner Selbstbestimmung ist in beiden Fällen ein Eingriff in die Grundrechte. Allerdings begründet diese nur gegenüber der staatlichen Gewalt ein unmittelbares Abwehrrecht. Gegenüber privaten Unternehmen muss der Gesetzgeber die konkurrierenden Grundrechtssphären des Unternehmens und des Betroffenen so abgrenzen, dass der eine seine Grundrechte nicht so ausübt, dass er dadurch die Grundrechte anderer verletzt.

Selbstbestimmung begründet kein eigentumsähnliches Herrschaftsrecht über personenbezogene Daten. Sie ist als Funktionsvoraussetzung einer freien und demokratischen Gesellschaft nicht in das – vom richtigen Preis abhängige – Belieben des Individuums als Händler seiner Daten gestellt. So „gehören“ etwa die Wartungsdaten eines Kraftfahrzeugs nicht nur dessen Eigentümer, sondern auch dem Reparaturbetrieb. Eine ausschließliche Zuordnung zu einem von beiden ist nicht möglich. Vielmehr ist eine Informations- und Kommunikationsordnung gefragt, die bestimmt, wer in welcher Beziehung befugt ist, mit den Daten in einer bestimmten Weise umzugehen. Diese Ordnung soll Kommunikation nicht unterbinden, sondern – allerdings selbstbestimmt – ermöglichen. Datenschutz bezweckt nicht den Schutz des Eigenbrötlers, der sich von der Welt abschotten will, sondern den Schutz desjenigen, der selbstbestimmt in der Gesellschaft

agiert und kommuniziert. Gesellschaftliche Einbindung aber setzt Kommunikation voraus und verpflichtet zu Kommunikation und damit in bestimmten Situationen auch zur Preisgabe personenbezogener Daten. Soweit überwiegende Allgemein- oder Individualinteressen es erfordern, ist auch eine Datenverarbeitung gegen den Willen des Betroffenen in einem verhältnismäßigen Umfang möglich. Diese Situationen zu bestimmen und zu regeln, ist jedoch Aufgabe des Gesetzgebers und Gegenstand des Datenschutzrechts.

Die USA haben kein Grundrecht auf informationelle Selbstbestimmung, sondern als „Privacy" nur ein „right to be left alone". Dementsprechend gibt es in USA nur einzelne Gesetze, die dieses Recht in bestimmten Lebensbereichen ansatzweise schützen. Eine allgemeine und systematische Gesetzgebung zum Schutz dieser spezifischen Form der Privatsphäre fehlt.

## Gefährdungen der Grundrechte

Diese Grundrechte werden durch aktuelle Entwicklungen dadurch gefährdet, dass unterschiedliche Akteure große Mengen sehr aussagekräftiger Daten sammeln und für vielfältige Zwecke – nicht zum Vorteil der Betroffenen – nutzen. Zum Teil sind die Betroffenen – zumindest formal – damit einverstanden, zum Teil aber werden die Daten ohne Wissen, Einwilligung oder Einfluss der Betroffenen gesammelt und genutzt.

Für viele Angebote im Internet besteht eine Kultur des „Umsonst". Jeder erwartet, dass diese nichts kosten. Suchmaschinen, Lexika, Filme, Bilder, Musik, Nachrichten, Zeitschriften, Social Networks, Foren und Blogs und viele andere Informationen und Dienstleistungen sollen „umsonst" verfügbar sein. Die Nutzer zahlen für die Nutzung zwar kein Geld, sie müssen sie aber in der neuen Währung personenbezogener Daten bezahlen. Social Networks verfolgen sogar gezielt das Geschäftsmodell, von möglichst vielen Nutzern möglichst viele personenbezogene Informationen zu erlangen, die sie für gezielte individuelle Werbung nutzen.

Diese Daten stehen aber nicht nur dem Plattformbetreiber zur Verfügung. Er gibt sie auch an „befreundete Unternehmen" weiter. Sie stehen außerdem grundsätzlich für jeden offen, der sich z. B. in einem sozialen Netzwerk anmeldet und die Daten – ohne Kontrolle – für die kommerzielle Weitergabe nutzt. Neu ist, dass die informationelle Selbstbestimmung nicht nur durch mächtige Institutionen (Staat, Presse, Auskunfteien), sondern durch die (Mit-)Nutzer selbst gefährdet wird. Im Web 2.0 kann jede Person Daten über andere weltweit preisgeben. Er kann sie damit auch vor aller Welt bloßstellen und ihren Ruf für alle Zeit ruinieren. Jeder kann zum Akteur, jeder kann zum Autor werden und dadurch auch – ungebremst und ungefiltert – in Persönlichkeitsrechte anderer eingreifen. Das gleiche Medium, das egalitäre Freiheit ermöglicht, schafft auch die Grundlage für ihre Gefährdung.

Die kostenlosen Angebote im Internet werden freiwillig genutzt. Sie bieten einen großen Nutzen und kosten kein Geld. Die Nutzer sind daher bereit, alle Geschäftsbedingungen und Datenschutzeinwilligungen ungelesen zu akzeptieren. Die damit verbundenen Risiken sind ihnen ansatzweise bewusst. Sie möchten sie nicht, schätzen aber die aktuellen Vorteile höher ein.

Im Regelfall sind die tatsächlichen Risiken jedoch viel höher, weil viele Unternehmen die gesetzlichen Grenzziehungen missachten oder – weil im Ausland – für sich nicht gelten lassen. So werden beispielsweise von vielen Websites oder Diensten nicht nur Cookies gesetzt, die die Kommunikation mit dem Nutzer unterstützen, sondern auch solche, die Informationen über ihn unbemerkt zu dritten Unternehmen leiten. Ein anderes Beispiel sind Apps, die sich auf dem Mobilfunkgerät viel mehr Rechte zuweisen lassen, als sie benötigen, und heimlich Daten der Kommunikation, der Aufenthaltsorte, der Adressbücher und der Kalender auslesen und an Dritte weiterleiten. Ein drittes Beispiel sind internetfähige Fernsehgeräte, die heimlich Daten über das Fernsehverhalten aufzeichnen und an den Hersteller übermitteln. Viele weitere Missbrauchsmethoden ließen sich hier aufzählen. Die Folge ist, dass in vielen Unternehmen Persönlichkeitsprofile über die Nutzer bestehen, von denen diese nicht wissen, dass es sie gibt und wofür sie verwendet werden. Sie wussten bis vor kurzer Zeit auch nicht, dass US-Geheimdienste alle Übertragungen im Internet überwachen und Daten ohne Anlass und ohne zeitliche Begrenzung speichern. Sie überwachen sogar in Deutschland alle Formen der Kommunikation, ohne dass dies den Betroffenen mitgeteilt wird und diese Möglichkeiten haben, sich dagegen zu wehren. Außerdem greifen sie auf alle Daten zu, die u.a. die Internetkonzerne Google, AOL, Microsoft, Apple, Skype und Facebook speichern, speichern diese ohne zeitliche Begrenzung und werten sie nach Belieben aus. Sie erhalten so Zugriff auf alle Daten, die von diesen vermittelten Kommunikationsinhalte wie E-Mails, Fotos, Chats, Videos, Videokonferenzen, Dateien, VoIP- oder GPS-Daten sowie auf die gesammelten Profile aller Nutzer. Sie können daher u.a. Geschäftsverbindungen, persönliche Beziehungen, Präferenzen und Einstellungen sowie individuelles Kommunikations- und Bewegungsverhalten nachvollziehen.

Nach dem „Foreign Intelligence Surveillance Act (FISA)" (50 U.S.C. § 1861) können US-Sicherheitsbehörden beim sogenannten FSI-Court eine Anordnung beantragen, die den Adressat verpflichtet, alle bei ihm gespeicherten Daten herauszugeben. Anordnungen haben nur zur Voraussetzung, dass die Daten mit einer Untersuchung von Terrorismus und Spionage in Verbindung stehen. Der FSI-Court ist ein geheim tagendes Sondergericht, dessen einzige Aufgabe es ist, über Anordnungen nach dem FISA zu entscheiden. Eine Anordnung kann von US-Unternehmen auch verlangen, dass sie Daten herausgeben, die sich im Ausland befinden oder die sie sich im Ausland (z. B. von Konzerntöchtern) beschaffen können. Weigern sie sich, drohen ihnen empfindliche Sanktionen. Der FISA bezweckt die Ausspähung von Nicht-US-Bürgern. Zur Herausgabe verpflichtet werden können aber nur Personen, die dem US-Recht unterliegen. Im Ergebnis unterliegt diesen Überwachungsmaßnahmen jeder, der

personenbezogene Daten einem amerikanischen Unternehmen oder dessen deutschen Töchtern anvertraut, auch wenn die Daten in Deutschland oder Europa gespeichert werden.

## Gesetzlicher Schutz

In der Europäischen Union gelten die Richtlinien für Datenschutz 95/46/EG und für Datenschutz in der elektronischen Kommunikation 2002/58/EG. Sie enthalten überwiegend sehr allgemeine und generische Regelungen, die durch die Mitgliedstaaten in innerstaatliches Recht umgesetzt worden sind. Beide Richtlinien gelten jedoch nicht für staatliche Überwachungsmaßnahmen der Mitgliedstaaten. In Deutschland sind die relevanten Regelungen grundsätzlich im Bundesdatenschutzgesetz (BDSG) zu finden. Für den Umgang mit Telekommunikationsdaten gilt das Telekommunikationsgesetz (TKG) (§§ 88 – 115) und für den Umgang mit Internetdaten das Telemediengesetz (TMG) (§§ 11 – 15a). Für die Überwachung durch deutsche Sicherheitsbehörden und Geheimdienste gibt es besondere Regelungen in den Gesetzen, die deren Tätigkeiten regeln.

Nach diesen Regelungen ist jeder Umgang mit personenbezogenen Daten ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung. Er soll daher soweit möglich vermieden werden (§ 3a BDSG). Zulässig ist er nur, wenn der Gesetzgeber oder der Betroffene ihn hinsichtlich Umfang und Zweck gebilligt haben (§ 4 Abs. 1 BDSG). Er muss dem Betroffenen gegenüber transparent gemacht werden, um ihm die Überprüfung der Rechtmäßigkeit und die Geltendmachung seiner Mitwirkungsrechte zu ermöglichen (§§ 4 Abs. 3, 33 und 34 BDSG). Der Umgang mit den Daten ist auf den gebilligten Zweck beschränkt und darf nur so weit und so lange erfolgen, wie dies für die Erreichung dieses Zwecks erforderlich ist (§§ 12 ff., 28 BDSG). Diese Grundsätze sind durch technisch-organisatorische Maßnahmen abzusichern (§ 9 BDSG). Dem Betroffenen stehen Mitwirkungsrechte und Rechte auf Schadensersatz zu (§§ 6 und 35, 7 und 8 BDSG). Die geschilderten Missbräuche von Internetunternehmen sind nach europäischem und deutschem Recht nicht zu rechtfertigen. Inwieweit die nachrichtendienstliche Ausspähung durch die NSA aufgrund von Geheimabkommen mit Deutschland zulässig ist, kann mangels Kenntnis dieser Abkommen nicht beurteilt werden. Das europäische und das deutsche Datenschutzrecht gelten jedoch nur, wenn die verantwortliche Stelle personenbezogene Daten in der Europäischen Union oder in Deutschland erhebt, verarbeitet oder nutzt (§ 1 Abs. 5 BDSG).

Werden die Daten im Ausland, beispielweise in den USA verarbeitet, gelten das europäische und das deutsche Datenschutzrecht nur insoweit, als beide einer verantwortlichen Stelle verbieten, personenbezogene Daten aus Deutschland oder Europa in ein Drittland zu übermitteln, wenn dort kein angemessenes Datenschutzniveau gewährleistet ist (Art. 25 DSRL und § 4b BDSG). In den USA besteht kein angemessenes Datenschutzniveau. Um dennoch einen Datenverkehr mit den USA zu ermöglichen, hat die Europäische Kommission die besondere Konstruktion des „Safe Harbor"-Abkommens gewählt. Danach dürfen Daten aus Europa an Organisationen in den USA übermittelt werden, wenn diese durch eine freiwillige Selbstverpflichtung ein angemessenes Datenschutzniveau erreichen und nachweisen. Das „Safe Harbor"-Abkommen erlaubt jedoch nicht die heimliche, unbefristete, anlasslose, massenhafte Speicherung personenbezogener Daten durch US-Sicherheitsbehörden. Sie liegt weit unterhalb eines angemessenen Datenschutzniveaus. Europäische Unternehmen, in denen US-Unternehmen einen bestimmenden Einfluss haben, geraten dadurch in eine Zwickmühle. Das US-Recht gebietet ihren „Müttern", personenbezogene Daten aus der Europäischen Union von ihren Töchtern zu beschaffen und an US-Sicherheitsbehörden zu übermitteln. Das europäische und deutsche Recht verbietet den „Töchtern", Daten zu diesem Zweck an die „Mütter" zu übermitteln. Übertragen Nutzer – wie etwa bei Social Networks – ihre Daten direkt an US-Unternehmen, gilt kein europäisches und kein deutsches Datenschutzrecht. Für diese Daten gilt dann nur US-Recht mit einem erheblich geringeren Datenschutzniveau.

## Schutzpflicht für Grundrechte

Jede Erhebung und Verwendung personenbezogener Daten ohne Kenntnis und Einwilligung des Betroffenen oder ohne gesetzliche Grundlage verletzt die Grundrechte auf informationelle Selbstbestimmung und Telekommunikationsgeheimnis. Die Grundrechte begründen eine Schutzpflicht des Staates. Nach ständiger Rechtsprechung des BVerfG muss er sich „schützend und fördernd vor die Grundrechte stellen" und Verletzungen verhindern (BVerfGE 121, 317, 356). Wie sie ihrer Schutzpflicht genügen, bestimmen Regierung und Gesetzgeber selbst. Hinsichtlich Auswahl der Mittel und Intensität des Schutzes haben sie einen großen Entscheidungsspielraum. Sie müssen jedoch gewährleisten, dass ein Untermaß des Schutzes nicht unterschritten wird (BVerfGE 88, 203, 254).

Für die Überwachung der Telekommunikation und des Internet hat das Bundesverfassungsgericht in seiner Entscheidung zur Vorratsdatenspeicherung (BVerfGE 125, 260, 307) festgestellt, dass sich Deutschland nicht zu einem Überwachungsstaat entwickeln darf. Die Freiheit ihrer Bürger, in ihrer Freiheitswahrnehmung nicht total erfasst und registriert zu werden, zählt „zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland". Daher stellt eine auf Telekommunikationsverkehrsdaten beschränkte, auf eine Speicherdauer von sechs Monaten begrenzte, von den Telekommunikationsanbietern vorgenommene dezentrale Speicherung, auf die Sicherheitsbehörden nur im Einzelfall nach Prüfung durch einen Richter Zugriff haben, die „Obergrenze" dessen dar, „was unter Verhältnismäßigkeitserwägungen rechtfertigungsfähig ist". Vor einem Mehr an Überwachung muss der deutsche Staat, müssen insbesondere Gesetzgeber und Bundesregierung die Bürger schützen.

Hierfür müssen beide geeignete Regelungen erlassen. Hierzu gehören etwa Vorgaben an verantwortliche Stellen in Deutschland, der Aufsichts-

behörde mitzuteilen, wenn sie von ihrem „Mutterunternehmen“ aufgefordert werden, personenbezogene Daten zu übermitteln, die nicht für die alltägliche Zusammenarbeit erforderlich sind. Notwendig ist aber auch, alle Geheimabkommen mit den USA, die im Zusammenhang mit dem Deutschlandvertrag 1955, der Notstandsverfassung 1968 und dem Zwei-Plus-Vier-Vertrag 1990 getroffen wurden, aus denen diese irgendwelche Rechte zur Überwachung in Deutschland ableiten könnten, zu kündigen.

Neben neuen Regelungen sind auch technisch-organisatorische Maßnahmen erforderlich, um die Grundrechte ausreichend zu schützen. Hierzu gehört, die Kontrolle von Praktiken des Datenumgangs zu verbessern. Die Aufsichtsbehörden müssen mit mehr Personal und mehr Kompetenzen und Zwangsmitteln ausgestattet werden, um missbräuchliche Praktiken besser aufzuspüren und abzustellen. Solche Maßnahmen bleiben allerdings auf Deutschland beschränkt.

## Allianz von Recht und Technik

In einer technischen Umgebung wie dem Internet ist Grundrechtsschutz auf eine technische Umsetzung angewiesen. Rechtliche Ziele können nur dann durchgesetzt werden, wenn sie auch in Technik abgebildet werden. Technischer Grundrechtsschutz hat gegenüber rein rechtlichem Schutz außerdem wesentliche Effektivitätsvorteile: Was technisch verhindert wird, muss nicht mehr verboten werden. Gegen Verhaltensregeln kann verstoßen werden, gegen technische Begrenzungen nicht. Datenschutztechnik kann so Kontrollen und Strafen überflüssig machen. Rechtlicher Schutz endet an den Grenzen Deutschlands oder Europas, Grundschutzrecht durch Technik wirkt dagegen global.

Informationelle Selbstbestimmung und Telekommunikationsgeheimnis müssen durch Infrastrukturen unterstützt werden, die ermöglichen, auf Gefährdungen automatisch zu reagieren, ohne dass dies aufdringlich oder belästigend wirkt. Die Erfüllung rechtlicher Vorgaben muss in die Techniksysteme integriert sein (Privacy by Design). Die Nutzer müssen über Techniken verfügen können, mit denen sie ihre Grundrechte selbst schützen können (Privacy Enhancing Technologies). Die Einhaltung von Verarbeitungsregeln zu kontrollieren, darf nicht die permanente persönliche Aufmerksamkeit erfordern, sondern muss automatisiert erfolgen. Die Durchsetzung von Zulassungs- und Verarbeitungsregeln muss im Regelfall durch Technik und nicht durch persönliches Handeln des Betroffenen erreicht werden. Wie dies möglich ist, zeigen die anderen Beiträge dieses Heftes.

Notwendig ist allerdings eine Methode, wie die nicht funktionalen rechtlichen Vorgaben, die meist sehr allgemein sind, in präzise funktionale technische Gestaltungsvorschläge umgesetzt werden können. Hierbei kann die Methode zur „Konkretisierung rechtlicher Anforderungen (KORA)“ helfen. Sie erreicht dieses Ziel in einem vierstufigen Begründungs- und Übersetzungsprozess. In einer ersten Stufe werden aus verfassungs- und einfachrechtlichen Vorgaben bezogen auf die spezifischen Chancen und Risiken der betreffenden Technik grundlegende rechtliche Anforderungen abgeleitet. Aus diesen Anforderungen können im zweiten Schritt Kriterien zur Bewertung und Gestaltung der zu betrachtenden technischen Systeme gewonnen werden, indem danach gefragt wird, welche allgemeinen Merkmale diese Techniksysteme erfüllen müssen, um die im ersten Schritt definierten Vorgaben zu erfüllen. Während Vorgaben und Kriterien in der Sprache des Rechts beschrieben werden, erfolgen die Schritte drei und vier in der Sprache der Technik. Im dritten Schritt werden zusammen mit Informatikern diese rechtlichen Vorgaben und Kriterien zu Gestaltungszielen konkretisiert, indem von der Technik her nach den Elementarfunktionen gefragt wird, die die Leistungsmerkmale des Techniksystems erfüllen müssen, um kriteriengerecht zu sein. Schließlich werden in einem letzten Schritt als Gestaltungsvorschläge die technischen und organisatorischen Lösungen ausgewählt, die diese technischen Ziele am besten erfüllen. KORA bietet eine strukturierte Vorgehensweise, um für jeden nachvollziehbar und daher auch für alle diskutierbar von allgemeinen normativen Vorgaben zu umsetzbaren Gestaltungsvorschlägen zu gelangen. Diese Konkretisierung kann auf weitere normative Vorgaben zur Sozialverträglichkeit erweitert werden. Im Projekt wurde aus ihr eine Methode entwickelt, sie um Vorgaben der Gebrauchstauglichkeit, der Vertrauenswürdigkeit und der IT-Sicherheit zu ergänzen.

## Fazit

Unternehmen und Geheimdienste gefährden die für Demokratie und Persönlichkeitsentwicklung essentiellen Grundrechte auf informationelle Selbstbestimmung und Telekommunikationsgeheimnis. Hiergegen muss der deutsche Staat seinen Bürgern Schutz gewähren. Dies erfordert insbesondere Techniken zu fördern, die geeignet sind, diese Grundrechte zu schützen.

**PROF. DR. ALEXANDER ROSSNAGEL**
Universität Kassel, Fachgebiet Öffentliches Recht mit dem Schwerpunkt Recht der Technik am Fachbereich Wirtschaftswissenschaften

## Literaturhinweise

David, K./ Geihs, K./Leimeister, J. M./ Roßnagel, A./Schmidt, L./Stumme, G./ Wacker, A. (Eds), Interdisciplinary Design of Socio-technical Ubiquitous Systems, Springer Verlag, Berlin u.a. 2014.

Dörfel, S./Hotho, A./Kartal-Aydemir, A./Roßnagel, A./Stumme, G.: Informationelle Selbstbestimmung im Web 2.0 – Chancen und Risiken sozialer Verschlagwortungssysteme, Springer Verlag, Berlin, Heidelberg 2013.

Roßnagel A./Moser-Knierim, A./Schweda, S.: Interessenausgleich im Rahmen der Vorratsdatenspeicherung – Analysen und Empfehlungen, Nomos Verlag, Baden-Baden 2013.

Roßnagel, A. (Hrsg.): Beck'scher Kommentar zum Recht der Telemediendienste, Kommentar zum TMG, SigG, SigV, JMStV, BGB (Auszüge), VwVfG (Auszüge), ZPO, Beck Verlag, München 2013.

Roßnagel A./Pfitzmann, A./Garstka, H.: Modernisierung des Datenschutzrechts, Gutachten für den Bundesinnenminister, Berlin 2001.

Gruppenbild der Ehrenden und Geehrten (v.l.): Dr. rer. nat. Ali Eren Culhaoglu, Dr.-Ing. Jakob Hoydis, Prof. Dr.-Ing. Christian Wietfeld, Prof. Dr.-Ing. Ingo Wolff (ITG-Vorsitzender), Sebastian Strunck (M.Sc.), Prof. Dr.-Ing. Albrecht Reibiger, Dipl.-Inf. Niklas Goddemeier, Dr.-Ing. Jens Ahrens, Dr.-Ing. Onur Hamza Karabey, Dr.-Ing. Martin Kördel, Dr.-Ing. Kai Daniel (nicht auf dem Bild Prof. Dr. phil. nat. Dietrich Wolf)

**PREISVERLEIHUNG**

# Ausgezeichnete Mitglieder

*Im Rahmen des VDE-Hauptstadtforums fand am 12.11. die Verleihung der ITG-Preise 2013 statt. Höhepunkt waren die Auszeichnungen zweier Mitglieder mit der VDE-Ehrenmedaille.*

Mit ihren Auszeichnungen ehrt die Fachgesellschaft sowohl außergewöhnliche Leistungen des akademischen Nachwuchses als auch das Werk herausragender Wissenschaftler. Der Ideenreichtum der ITG-Mitglieder und die praxisnahen Entwicklungen der Informations- und Kommunikationstechnik sollen auf diese Weise besondere Anerkennung erfahren.

Bei der Verleihung Mitte November in Berlin wurden Preise in mehreren Kategorien vergeben. Sechs Mitglieder wurden mit dem ITG-Preis für hervorragende Veröffentlichungen ausgezeichnet. So wurde Dr.-Ing. Jens Ahrens für sein Buch „Analytic Methods of Sound Field Synthesis“ geehrt. Bei der Schallfeldsynthese wird ein Ensemble von Lautsprechern derart angesteuert, dass die Felder der Lautsprecher sich überlagern, und ein Schallfeld mit einer gewünschten physikalischen Struktur entsteht. Das Buch „Analytic Methods of Sound Field Synthesis“ behandelt das Thema mit Fokus auf der Audiowiedergabe. Die Veröffentlichung von Jens Ahrens, der aktuell bei Microsoft Research in Redmond in den USA forscht, kann bereits heute als Standardwerk der 3D-Audioverarbeitung für Lehre und Forschung bezeichnet werden.

Ausgezeichnet wurden auch Dr.-Ing. Onur Hamza Karabey und Sebastian Strunck, beide am Institut für Mikrowellentechnik und Photonik an der Technischen Universität Darmstadt tätig. In ihrem Aufsatz „A 2-D Electronically Steered Phased-Array Antenna with 2x2 Elements in LC Display Technology“ beschreiben sie eine neue Technologie zur Realisierung von variablen Verzögerungsleitungen für ein elektronisch phasengesteuertes Antennenarray. Durch einen neuartigen Aufbau und die Verwendung der bei Flüssigkristallanzeigen seit Langem bewährten LCD-Technik ist es ihnen gelungen, erstmalig eine in zwei Dimensionen elektronisch schwenkbare Antenne mit äußerst dünnem Profil zu entwickeln. Damit haben sie einen wesentlichen Fortschritt in Richtung der kostengünstigen Herstellung von größeren Arrays erzielt, die sowohl für den mobilen

Einsatz bei terrestrischen Übertragungssystemen als auch der Satellitenkommunikation im Mikrowellenbereich hervorragend geeignet sind.

Prof. Dr.-Ing. Christian Wietfeld, Leiter des Lehrstuhls für Kommunikationsnetze an der TU Dortmund, Dipl.-Inf. Niklas Goddemeier, der an diesem Lehrstuhl tätig ist, und Dr.-Ing. Kai Daniel von der RWE Deutschland AG in Essen haben gemeinsam den Aufsatz „Role-Based Connectivity Management with Realistic Air-to-Ground Channels for Cooperative UAVs“ verfasst. In ihm geht es um die selbstorganisierte Optimierung der Mess- und Erkundungsabdeckung eines hochmobilen, fliegenden Roboterschwarms. Die unbemannten Fluggeräte unterstützen Rettungseinsätze und können für verteilte Umweltmessungen bei gleichzeitiger Einhaltung von Kommunikationsanforderungen eingesetzt werden.

## Herausragende Dissertationen

Der ITG-Förderpreis für ausgezeichnete Dissertationen wurde 2013 drei Mal verliehen. Einer der Preisträger ist Dr. rer. nat. Ali Eren Culhaoglu vom Deutschen Zentrum für Luft- und Raumfahrt e.V. (DLR) in Weßling für seine Arbeit „Microwave Metamaterials: Superlensing and Design of Low Reflection Coatings“. Sie widmet sich dem relativ neuen Forschungsgebiet der „Metamaterialien“, Materialien also, die gezielt dünn und leicht entworfen und hergestellt werden, um elektromagnetische Wellen für einen definierten Frequenzbereich z.B. sehr stark zu absorbieren. Dr. Culhaoglu hat nun solche Metamaterialien entwickelt und ihr Verhalten in aufwendigen Simulationen optimiert.

Dr.-Ing. Jakob Hoydis von der Alcatel-Lucent Deutschland AG, Bell Labs Germany in Stuttgart hat sich in seiner Dissertation „Random Matrix Methods for Advanced Communication Systems“ mit der Analyse und Optimierung „dichter“ Funknetze beschäftigt, die durch eine sehr große Anzahl von Benutzern, Basisstationen und Antennen charakterisiert sind. Ein großer Teil der Arbeit befasst sich mit der Theorie großer Zufallsmatrizen, die eine vereinfachte Analyse komplexer Systeme ermöglicht.

Dritter Preisträger in dieser Kategorie ist Dr.-Ing. Martin Kördel von der Siemens AG in München. In seiner Arbeit präsentiert er ein neuartiges berührungsloses und ortsauflösendes Inspektionsverfahren für großflächig aufgebrachte planare elektronische Funktionseinheiten. Das Verfahren beruht auf kapazitiver Kopplung und eignet sich in idealer Weise zur Inspektion der unterschiedlichen Funktionseinheiten von Flat-Panel-Displays, E-Book-Readern sowie gedruckten Sensoren bzw. Schaltungen.

## Die Ehrenmedaillen

Die VDE-Ehrenmedaille für besondere Verdienste für die Fachgesellschaft wurde in diesem Jahr an zwei Persönlichkeiten überreicht: An Prof. Dr.-Ing. Albrecht Reibiger und Prof. Dr. phil. nat. Dietrich Wolf. In mehr als 50 Jahren, in denen sich Prof. Reibinger mit der Elektrotechnik und insbesondere mit der Netzwerktheorie und Schaltungssimulation an der TU Dresden befasst hat, hat er die Entwicklung auf diesen Gebieten mit zahlreichen grundlegenden Beiträgen bereichert. Darüber hinaus war er auch immer in Gremien seiner Wissenschaft tätig, wo er sich insbesondere um die Neuausrichtung der Lehre und um die Förderung des wissenschaftlichen Nachwuchses verdient gemacht hat. So war es nur konsequent, dass er aufgrund seiner umfassenden und tiefgründigen Kenntnisse auf dem Gebiet der Elektrotechnik in Gremien der ITG mitgearbeitet hat. Der Fachausschuss 8.4 „Integrierte Systeme“ hat von seiner Mitarbeit außerordentlich profitiert. Im ITG-Vorstand ist er zusammen mit Prof. Dr. D. Wolf seit vielen Jahren für Preise und Ehrungen zuständig. Dabei hat er sich mit großem Aufwand mit der Begutachtung von Beiträgen junger Wissenschaftlerinnen und Wissenschaftler befasst und so manchen Rohdiamanten ans Licht gebracht.

Prof. Dr. phil. nat. Dietrich Wolf hat sich in seiner langjährigen Tätigkeit am Fachbereich Physik der Frankfurter Johann-Wolfgang-Goethe-Universität als hervorragender Hochschullehrer und Wissenschaftler erwiesen, dessen Arbeiten weithin international Anerkennung gefunden haben. Er gilt als ein herausragender Experte auf dem Gebiet der Fluktuationsphänomene, der Theorie stochastischer Prozesse, der Informations- und der Signaltheorie. Vorangetrieben hat er auch die Entwicklung von Sprachcodierungs- und Spracherkennungsverfahren. In besonderer Weise hat sich Prof. Wolf seit Beginn seiner Mitgliedschaft im Jahr 1970 im VDE/NTG/ITG für diesen Themenkreis eingesetzt. Hervorzuheben ist seine Mitarbeit im Fachausschuss 1 „Informations- und Signaltheorie“ ab 1976. Zu erwähnen ist auch die maßgebliche Beteiligung an der Neustrukturierung der ITG-Fachbereiche und -Fachausschüsse. Als Mitglied des ITG-Vorstands im Zeitraum von 1991 bis 1996 hat er die Einrichtung des ITG-Förderpreises vorgeschlagen und durchgesetzt.

Prof. Reibinger (links) und Prof. Wolf

## Zwei Ehrenurkunden

Mit der VDE-Ehrenurkunde für ihr hohes ehrenamtliches Engagement wurden Prof. Dr.-Ing. Christian Schäffer und Dr.-Ing. Volker Wittpahl ausgezeichnet. Prof. Schäffer für sein hohes ehrenamtliches Engagement als langjähriger Leiter der ITG-Fachgruppe 5.3.1 „Modellierung photonischer Komponenten und Systeme“ und die stetige Fortentwicklung der Fachtagung Photonische Netze als wissenschaftlicher Tagungsleiter; Dr.-Ing. Wittpahl für sein hohes ehrenamtliches Engagement als langjähriger Leiter des ITG-Fachbereichs 2 „Dienste und Anwendungen“ und die stetige Fortentwicklung neuer Themen sowie sein herausragendes Engagement bei vielen ITG-Veranstaltungen. Die Auszeichnungen wurden und werden in den jeweiligen Gremiensitzungen überreicht.

FACHGRUPPE 5.3.1

## WORKSHOP ZU OPTISCHEN MULTIPLEXTECHNIKEN

Im Rahmen von regelmäßig stattfindenden Workshops treffen sich Vertreter der einschlägigen Industrieunternehmen sowie der auf dem Gebiet der optischen Nachrichtentechnik tätigen Hochschulen und Forschungseinrichtungen zum intensiven Erfahrungsaustausch. Diese Workshops werden abwechselnd von den Mitgliedern der Fachgruppe „Modellierung und Simulation photonischer Komponenten und Systeme“ organisiert und bieten ein Forum zur Diskussion aktueller Fragestellungen der optischen Übertragungstechnik. Ein aktuelles Rahmenthema verbindet die Beiträge der zwei halbtägigen Vortragsblöcke, in denen besonders auch jungen Nachwuchswissenschaftlern die Möglichkeit gegeben wird, ihre aktuellen Forschungsergebnisse zu präsentieren und diese mit Fachleuten aus der Industrie und Wissenschaft zu diskutieren. Der nächste Workshop ist für Donnerstag, den 20. und Freitag, den 21. Februar geplant. Unter dem Rahmenthema „Optische Multiplextechniken“ wird das Treffen in den Räumen der T-Labs in Berlin stattfinden. Interessenten können sich für die E-Mail-Verteilerliste der Fachgruppenworkshops unter https://lists.fau.de/cgi-bin/listinfo/itg531-workshop registrieren oder sich an den Leiter der Fachgruppe wenden (Bernhard.Schmauss@fau.de).

FOKUSPROJEKT

## FRESCO – FUTURE RELIABLE AND SECURE COMMUNICATIONS

Die allgegenwärtige Nutzbarkeit von Kommunikations- und Informationssystemen sowie elektronischer Medien ist die Voraussetzung für viele Prozesse in der modernen Gesellschaft. Eine perfekt funktionierende Infrastruktur wird mit großer Selbstverständlichkeit als verfügbar vorausgesetzt. Besondere Bedeutung erlangen zuverlässige, hoch verfügbare und sichere Kommunikationssysteme in Zukunftsanwendungen wie Industrie 4.0, Smart City, in intelligenten Transport- und Logistiksystemen sowie dem Smart Grid. Der Vorstand der ITG hat beschlossen, den beschriebenen Themenkomplex im Rahmen des Fokusprojekts „Fresco – Future Reliable and Secure Communications“ gebündelt zu bearbeiten. Dieses Projekt hat die Aufgabe, die bereits in der ITG und ihren Fachausschüssen vorhandenen vielfältigen Aktivitäten zu bündeln und auszubauen. Damit soll der Informationsaustausch zwischen den Fachleuten gestärkt und eine Diskussionsplattform auch für den politischen Dialog gebildet werden. Als erste öffentliche Aktivität wird am 25. Februar 2014 in Berlin der eintägige öffentliche Workshop „Zuverlässige und sichere Kommunikation“ veranstaltet. Hochrangige eingeladene Experten aus Industrie, Politik und Forschung werden Teilaspekte der Fragestellung in Fachbeiträgen vorstellen und diskutieren. Interessierte Mitglieder des VDE sind hierzu herzlich eingeladen. Weitere Informationen sind auf der Webseite der ITG verfügbar. Da die Teilnehmerzahl begrenzt ist, empfiehlt sich eine frühzeitige Anmeldung.

FACHGRUPPE 9.4.1

## TAGUNG DER GRUPPE STROMVERSORGUNG IN HAMBURG

Die Tagung der Fachgruppe 9.4.1 „Stromversorgung“ im zweiten Halbjahr 2013 fand dieses Mal anläßlich der INTELEC® 2013 statt, der 35. Internationalen Telekommunikations- und Energiekonferenz im Kongresscenter Hamburg. Die Teilnehmer der Fachgruppe nahmen am 16. Oktober am abendlichen Konferenzdinner in der alten Hagenbeck’schen Dressurhalle in Hamburg teil. Dabei wurden bereits Strategien für das weitere Vorgehen der Fachgruppe und die nächste Tagung besprochen. Am 17. Oktober versammelten sich 14 Teilnehmer der Fachgruppe, bestehend aus Geschäftsführern namhafter Firmen, Herausgebern von Fachpublikationen sowie Topentwicklern. Sie tauschten in einer umfangreichen Tagesordnung mit hervorragenden Präsentationen gegenseitig Erfahrungen aus. Der Geschäftsführer der ITG, Dr. Volker Schanz, informierte über die anstehenden Neuwahlen des ITG-Vorstandes und wies auf verschiedene Aktivitäten für das Jahr 2014 der ITG hin, vor allem auf die Tagung „Sicherheit und Zuverlässigkeit“ am 25. Februar 2014. Dabei wurde außerdem deutlich, dass der VDE seinen Sachverstand auch bei den Fraktionen im Deutschen Bundestag einbringt, um hier zum Beispiel das vorhandene Know-how im Bereich der Energiewende weiterzugeben.

Ein wichtiges Thema war der Vortrag von Dr. Manfred Schlenk, General Manager NMB-Minebea, der über seine Erfahrungen bei der Produktion in China berichtete. Dabei zeigte sich insbesondere, dass Präsenz vor Ort und Vorkehrungen gegen Fachkräfteabwanderung wichtige Themen sind. Das Thema „Sicherheitsnormung für Lithium-Ionen-Batterien“ von Dipl.-Ing. Ulrich Krieger, DKE Referat K371, zeigte auf, dass im Bereich der Normung in Bezug auf Verwendung sowie den Transport von Lithium-Ionen-Batterien Handlungsbedarf besteht. Dies ist erkannt und Normen sind in Bearbeitung.

Normen für die Speicherung elektrischer Energie aus der Photovoltaik im Haushaltsbereich mithilfe von Lithium-Batterien sind ebenfalls ein wichtiges Thema. Nach seinen Ausführungen kosten Batteriepacks von Lithium-Ionen-Batterien derzeit etwa 500 Euro pro Kilowattstunde, was sich bis 2020 halbieren dürfte. An die Speicherung elektrischer Energie knüpfte der Vortrag von Dipl.-Phys. Karen Derendorf an. Sie ist Projektleiterin Abteilung Energiespeicher bei Next Energy in Oldenburg. In umfangreichen Untersuchungen wurden hier Vergleiche zwischen der Speicherung in Bleibatterien und Lithium-Ionen-Batterien vorgenommen, Wirtschaftlichkeitsrechnungen angestellt und Sicherheitsfragen beantwortet.

Innerhalb der Fachgruppe sind drei Arbeitsgruppen eingerichtet, die sich mit speziellen Themen beschäftigen. Bernhard Böden, Geschäftsfüh-

rer von Power Innovation in Achim, Leiter der Arbeitsgruppe „Technologien zur Speicherung elektrischer Energie“, berichtete über seine Zusammenarbeit mit der Telekom, die enorme Speicherkapazitäten in ihren Vermittlungsanlagen zur Kurzzeitlieferung elektrischer Energie ins öffentliche Netz zur Verfügung stellen könnte. Dr. Manfred Schlenk, General Manager NMB-Minebea, beschäftigte sich als Vorsitzender der Arbeitsgruppe 2 mit der Energieoptimierung, der digitalen Regelung und Sicherheit. In umfangreichen Forschungen und Entwicklungen ist es gelungen, die geforderte Stand-by-Leistung von unter 0,5 W erheblich zu verringern. Um Bauelementeströme zu verfolgen und dadurch Produktionsdaten und Herstellerinformationen zu bekommen, war der Vortrag von Herrn Alexander Gerfer, dem Leiter des internationalen Produktmanagements der Firma Würth Elektronik eiSos, ein hervorragendes Thema.

Hervorzuheben sind drei wesentliche Aussagen. Erstens: Die Chance in Deutschland besteht darin, Innovationen hervorzubringen, um mit China mithalten zu können. Zweitens: In China werden Unternehmen staatlich gefördert, was den Wettbewerb erschwert. Drittens: Der Einsatz der Elektronik in Autos wird zunehmen. Es zeigte sich, dass neue Innovationen im Bereich von Handys und Computern bisher bekannte Marken, die Produkte mit diesen Innovationen nicht vertreiben, schwer belasten.

Es wird angestrebt, die nächste Tagung der Fachgruppe Anfang 2014 in Portugal stattfinden zu lassen, um aus eigener Anschauung die dortige Entwicklung erleben zu können. Die Fachgruppe ist offen für weitere Mitglieder, die sich vorstellen können, wichtige Informationen zu erhalten, um dadurch wertvolle Hinweise für ihre Arbeit im Unternehmen gewinnen zu können.

**PROF. DIPL.-ING. MANFRED DORSCH**
Steinbeis-Transferzentrum Angewandte Elektronik
an der Hochschule Heilbronn,
manfred.dorsch@hs-heilbronn.de

# Personalia

## NEU GEWÄHLTE SPRECHER VON ITG-FACHAUSSCHÜSSEN UND -GRUPPEN

1

2

3

### 1 +++ PROF. DR.-ING. DIRK HEBERLING

**RWTH Aachen, Institut für Hochfrequenztechnik**

Prof. Heberling ist zum 1. Januar 2014 zum neuen Sprecher des ITG-Fachausschusses 7.1 „Antennen“ gewählt worden. Er ist seit 2008 Leiter des Lehrstuhls und Instituts für Hochfrequenztechnik der RWTH Aachen und beschäftigt sich dort unter anderem mit Antennen und Antennenmesstechnik. Er studierte und promovierte an der RWTH Aachen. Von 1995 bis 2008 war er Abteilungsleiter bei der IMST GmbH in Kamp-Lintfort, zunächst zuständig für die Abteilung Antennen und Elektromagnetische Umweltverträglichkeit (EMVU), später für die Abteilung Informations- und Kommunikationssysteme. // **www.ihf.rwth-aachen.de**

### 2 +++ DR. PETER KNOTT

**Fraunhofer-Institut für Hochfrequenzphysik und Radartechnik (FHR), Wachtberg**

Dr. Knott ist zum stellvertretenden Sprecher des ITG-Fachausschusses 7.1 „Antennen“ gewählt worden. Im Anschluss an sein Studium der Elektrotechnik an der RWTH Aachen begann er 1994 seine Tätigkeit beim Fraunhofer-Institut für Hochfrequenzphysik und Radartechnik FHR (ehemals FGAN) in Wachtberg. Seine Forschungsarbeit konzentrierte sich auf die elektromagnetische Simulation und Entwicklung von Antennengruppen für Radarsysteme. Im Jahr 2001 schloss er seine Promotion auf dem Gebiet der elektromagnetischen Modellierung und Diagrammformung für große Antennengruppen ab. Seit 2005 leitet er die Abteilung Antennentechnologie und elektromagnetische Modellierung (AEM) des FHR. Dr. Knott ist zurzeit Vice Chair im Executive Committee des IEEE MTT/AP Joint Chapter und Mitglied der ICT COST Action IC1102 Versatile, Integrated, and Signal-aware Technologies for Antennas (VISTA). Er übt außerdem eine Lehrtätigkeit im Fach „Antenna Engineering“ an der RWTH Aachen aus.

### 3 +++ DR. JOACHIM SACHS

**Ericsson, Stockholm**

Dr. Sachs ist zum Leiter des ITG-Fachausschusses 5.2 „Kommunikationsnetze und -systeme“ gewählt worden. Dessen Leitung nimmt er gemeinsam mit Prof. Christian Wietfeld wahr. Seit 1997 ist Joachim Sachs bei Ericsson in der zentralen Forschung tätig, zunächst in Aachen und seit 2011 in Stockholm. Er studierte Elektrotechnik in Aachen, Toulouse, Trondheim und Glasgow und promovierte an der TU Berlin. In 2009 war er Gastwissenschaftler an der Stanford University. Joachim Sachs ist seit 1998 in der ITG aktiv und hat in den Fachgruppen 5.2.3 und 5.2.1 sowie dem Fachausschuss 5.2 mitgewirkt.

## Veranstaltungen

**Hinweis: Andere interessante Veranstaltungen sind auf den Seiten 46 und 47 des VDE dialog angekündigt.**

**20.– 21.02.2014, Berlin**
**ITG-Fachgruppenworkshop „Optische Multiplextechniken“**
ITG FG 5.3.1
**// lists.fau.de/cgi-bin/listinfo/itg531-workshop**

**23.– 25.02.2014, Kloster Banz**
**26. Workshop „Testmethoden und Zuverlässigkeit von Schaltungen und Systemen“ (TuZ 2014)**
ITG FG 8.2, GMM, GI
**// www.vde.com**

**25.02.2014, Berlin**
**ITG-Workshop „Zuverlässige und sichere Kommunikation“**
ITG FP-Gruppe
**// www.vde.com/itg**

**10.– 12.03.2014, Böblingen**
**17. Workshop Methoden und Beschreibungssprachen zur Modellierung und Verifikation von Schaltungen und Systemen (MBMV 2014)**
ITG FG 8.2.3 + 8.2.4, GMM, GI
**// www-05.ibm.com/de/entwicklung/mbmv2014/index.html**

**10.–13.03.2014, Oldenburg**
**DAGA: 40. Jahrestagung für Akustik**
DEGA, ITG FB 4
**// daga2014.de**

**17.– 19.03.2014, Bamberg**
**17th Int. Conference on Measurement, Modeling, and Evaluation of Computer and Communication Systems and Dependability and Fault Tolerance (MMB & DFT 2014)**
ITG FA 6.5 + 6.3, GI
**// www.mmb2014.de**

**05.– 06.05.2014, Leipzig**
**15. ITG-Fachtagung Photonische Netze 2014**
ITG FA 5.3
**// www.vde.com/Photonische-Netze2014**

**21.– 22.05.2014, Osnabrück**
**19. ITG-Fachtagung Mobilkommunikation**
TG FB 5, BV Osnabrück, FH Osnabrück
**// www.mobilkomtagung.de/fachtagungmobilkommunikation.html**

**01.– 03.06.2014, Berlin**
**World Telecommunications Congress (WTC 2014): Enabling Infrastructure for the Future**
ITG
**// www.wtc2014.de**

**02.– 04.06.2014, München**
**Joint conference of the 45th International Symposium on Robotics (ISR 2014) and the 8th German Conference on Robotics (ROBOTIK 2014)**
IFR, DGR, ITG
**// conference.vde.com/isr2014**

**03.– 04.06.2014, Nürnberg**
**17. ITG/GMA-Tagung „Sensoren und Messsysteme“**
ITG, GMA
**// www.vde.com/sensoren2014**

**03.– 05.06.2014, Berlin**
**10th European Conference on Synthetic Aperture Radar (EUSAR 2014)**
ITG FA 7.1, 7.4, DLR
**// www.eusar.de**

**22.– 26.06.2014, Dresden**
**27th Int. Conference on Electrical Contacts (ICEC 2014)**
ITG, ETG
**// www.icec2014.org**

## Call for Papers

**05.– 08.05.2014, Köln**
**26. Fachtagung der Fernseh- und Kinotechnischen Gesellschaft (FKTG): Die Medienwelt von morgen – größer, schöner, überall und jederzeit**
Die FKTG will Wissenschaftlern, Entwicklern und Anwendern der TV-, Film- und Medienbranche auf der Tagung 2014 ein Forum bieten und über die aktuellen Erkenntnisse aus Forschung, Technologie und Anwendung informieren. Die Einsendefrist endet am 17. Januar 2014
**// www.fktg.org/koeln2014**

**01.– 02.07.2014, Dortmund**
**Smart SysTech 2014: European Conference on Smart Objects, Systems and Technologies**
Full paper submission until 7th of February 2014. Accepted contributions will be published in the VDE conference proceedings and in the IEEE Xplore® Digital Library. Topics of Interest e.g. Smart Objects and Technologies, Smart Objects and Communication, Industry 4.0.
**// www.smart-systech.eu/**

**07.– 10.09.2014, Berlin**
**4th IEEE International Conference on Consumer Electronics – Berlin (IEEE 2014 ICCE-Berlin)**
The Conference will bring together researchers and engineers from industry, research centers and academia to exchange information and results of recent work on systems, circuits, technologies, processes and applications in the field of consumer electronics. The Call for Papers is available. Please submit your paper abstract until March 10.
**// www.icce-berlin.org**

**24.– 26.09.2014, Erlangen**
**Speech Communication, ITG-Fachtagung Sprachkommunikation**
Themen sind u.a. Signalverbesserung, Sprachübertragung, instrumentelle Sprachqualitätsmaße, automatische Sprach- und Sprechererkennung und Sprachdialogsysteme. Besondere Aufmerksamkeit gilt der Sprachverarbeitung zur Mensch-Maschine-Kommunikation. Für akzeptierte Beiträge ist eine Veröffentlichung via IEEE Xplore vorgesehen. Sie sollten als 4-seitiger Artikel (inkl. aller Referenzen) in englischer Sprache verfasst sein. Einreichungen sind bis zum 11.04.2014 möglich.
**// www.lms.lnt.de/itgspeech2014/**

**29.09.– 03.10.2014, Berlin**
**25th European Symposium on Reliability of Electron Devices (ESREF 2014)**
The Conference will strongly connect with Europe's industry of electronic devices, ranging from state of the art IC technology to the heart of Europe's industry, power devices. It will have a special focus on organic/polymer electronic devices. Deadline: March 14.
**// www.esref2014.org**

## Impressum

**ITG-news**

Herausgeber: Informationstechnische Gesellschaft im VDE, Frankfurt am Main

Redaktion: Dr. Volker Schanz, Christina Gaußmann

Telefon: 069/6308-360/-362
E-Mail: itg@vde.com
Internet: www.vde.com/itg

Konzept und Realisation: HEALTH-CARE-COM GmbH, ein Unternehmen des VDE Verlags GmbH, Hans-Peter Bröckerhoff, Christian Sälzer, Martin Wolczyk

Druck: Heenemann GmbH & Co. KG, Berlin