

Jahresbericht 2013

Inhaltsverzeichnis

Personelle Zusammensetzung	2
Kurzbeschreibung des Lehrstuhls	3
Lehrveranstaltungen	4
Wintersemester 2012/2013.....	4
Sommersemester 2013	4
Wintersemester 2013/2014.....	4
Forschungsprojekte	5
Sensoren für eine kooperative Netzüberwachung.....	5
PADIOFIRE (Parallelisierte Anwendungserkennung in Overlaynetzen) - Teilvorhaben Signatursprache für Web 2.0-Protokolle sowie zugehörige Parser	5
vmFIRE (Firewalling in virtuellen Maschinen) - Teilvorhaben Entwicklung eines Redirektormoduls und Analyse von Migrationsstrategien und –verfahren bei Virtuellen Maschinen	6
Studie zur Sicherung der IT-Sicherheit von Prozessrechnersystemen	7
P2P Intrusion Detection	7
UML-basierte Entwicklung von Kommunikationsprotokollen.....	8
BTU International Graduate School, ZUSYS (Dependable Hardware / Software Systems). 8	
Veröffentlichungen.....	9
Vorträge.....	11
Dissertationen, Diplom-, Bachelor- und Studienarbeiten	13
Dissertationen.....	13
Diplomarbeiten.....	13
Masterarbeiten.....	13
Bachelorarbeiten.....	13
Mitarbeit in Gremien	14
Rechnerausstattung.....	15
Auszeichnungen	16
Sonstiges.....	17

Personelle Zusammensetzung

Lehrstuhlleiter:	Prof. Dr.-Ing. habil. Hartmut König	
Adresse:	Brandenburgische Technische Universität Cottbus Fakultät 1, Institut für Informatik Lehrstuhl Rechnernetze und Kommunikationssysteme PF 10 13 44 03013 Cottbus	
Telefon:	03 55 / 69 22 36	
Fax:	03 55 / 69 21 27	
E-Mail:	koenig@informatik.tu-cottbus.de	
WWW:	http://www-rnks.informatik.tu-cottbus.de/	
Sekretärin:	Katrín Willhöft	
Akademische Mitarbeiter:	M.Sc. Michael Kirsche M.Sc. Andreas Paul Dipl.-Inf. Michael Vogel	seit 01.07.2013
Projektmitarbeiter:	Dipl.-Inf. Jan Gäbler Dipl.-Inf. Ronny Klauck M.Sc. Andreas Paul M.Sc. René Rietz M.Sc. Franka Schuster	bis 30.06.2013
Technischer Mitarbeiter:	Dipl.-Inf. Joachim Paschke	
Doktoranden:	B.Sc. Radoslaw Cwalinski M.Sc. Prabhu Shankar Kaliappan M.Sc. Stefanie Judith Opitz Dipl.-Inf. Mario Pink	

Kurzbeschreibung des Lehrstuhls

Der Lehrstuhl *Rechnernetze und Kommunikationssysteme* beschäftigt sich mit Gestaltungsprinzipien moderner Kommunikationssysteme und verteilter Anwendungen. Ziel der Forschungsarbeiten ist die Entwicklung neuer Konzeptlösungen und ihre Erprobung in Prototypimplementierungen. Die Forschungsarbeiten umfassen sowohl theoretische als auch praktische Untersuchungen. Es werden folgende Forschungsschwerpunkte bearbeitet:

(1) Mobile kollaborative Systeme

- Gruppenkommunikation in mobilen Umgebungen
- Handover-Techniken
- Lokalisierung von Systemen und Personen
- Wireless Personal Networks (IEEE 802.15)
- Plattformen für die Unterstützung mobiler kollaborativer Anwendungen

(2) IT-Sicherheit / Netzmonitoring

- Peer-to-Peer Intrusion Detection
- Signaturableitung und -validation
- Web-Sicherheit
- Monitoring von Virtuellen Maschinen

(3) Protocol Engineering

- UML-basierte Protokollentwicklung
-

Lehrveranstaltungen

Wintersemester 2012/2013

- Vorlesung "Rechnernetze und Kommunikationssysteme I"
- Praktikum "Rechnernetze und Kommunikationssysteme"
- Vorlesung "Innovative Netztechnologien"
- Vorlesung "IT-Sicherheit"
- Seminar/Praktikum "Mobile kollaborative Anwendungen"
- Oberseminar

Sommersemester 2013

- Vorlesung "Rechnernetze und Kommunikationssysteme II"
- Fortgeschrittenenpraktikum "Rechnernetze und Kommunikationssysteme"
- Seminar „IT-Sicherheit in kritischen Infrastrukturen“
- Praktikum/Seminar „Internet der Dinge“
- Proseminar "Trends in Kommunikationstechnologien"
- Oberseminar

Wintersemester 2013/2014

- Vorlesung "Grundlagen der Rechnernetze"
 - Praktikum "Grundlagen der Rechnernetze"
 - Vorlesung "Protocol Engineering"
 - Projektseminar "Netzwerksimulation"
 - Oberseminar
-

Forschungsprojekte

Sensoren für eine kooperative Netzüberwachung

BMBF-Programm ForMaT "Forschung für den Markt im Team" Phase II
(gemeinsames Projekt mit dem *IHP Frankfurt (Oder)* und dem Lehrstuhl *ABWL und das Besondere des Marketings und des Innovationsmanagements*)

01.04.2011 - 31.03.2013

Jan Gäbler, Ronny Klauck, Andreas Paul, Franka Schuster, Michael Sprejz, Hartmut König

Ziel des gemeinsam mit dem IHP Frankfurt (Oder) bearbeiteten Projekts ist es, ausgehend von den Anforderungen an den Schutz von industriellen IT-Systemen, ein ganzheitliches Konzept für die Gestaltung von Sicherheitslösungen für industrielle kritische Infrastrukturen (KRITIS) in Form einer verteilten und reaktiven Sicherheitsplattform zu schaffen. Dazu sollen Netzsensoren entwickelt werden, die ein Monitoring-Overlaynetz bilden, das die kritische Infrastruktur überwacht. Es wird die Entwicklung unterschiedlicher Sensortypen angestrebt, die sowohl für die Überwachung von Festnetzen als auch von Netzen der drahtlosen Kommunikation eingesetzt werden können. Die Monitoring-Sensoren sollen konfigurierbar sein, um sie mit Fähigkeiten zur Erfassung und Analyse von Netzwerkdaten auszustatten, die den Erfordernissen des jeweiligen Anwendungsfalls entsprechen. Als konkreter Anwendungsfall werden SCADA (*Supervisory Control and Data Acquisition*) – Systeme für Automatisierungsanwendungen und Industrielle Prozessleit- und Steuersysteme betrachtet.

PADIOFIRE (*Parallelisierte Anwendungserkennung in Overlaynetzen*) - Teilvorhaben Signatursprache für Web 2.0-Protokolle sowie zugehörige Parser

BMBF-Verbundvorhaben
(gemeinsames Projekt mit der *Friedrich-Alexander-Universität Erlangen-Nürnberg* und der *genua (Gesellschaft für Netzwerk- und UNIX-Administration) mbH Kirchheim*)

01.07.2011 - 30.06.2013

René Rietz, Hartmut König

Die wachsende Durchdringung von Internet-Technologien in eine immer größer werdende Zahl von Anwendungsbereichen bringt ein stetig zunehmendes Bedrohungspotential für damit verbundene Systeme mit sich. Des Weiteren stellt die Realisierung immer neuer Dienste über das Internet, einschließlich der Integration klassischer Dienste und Netze wie Telefonie und Audio/Video-Broadcasting, hohe Anforderungen an die Kommunikationsinfrastruktur selbst, aber vor allem auch an die Sicherheit. Für die Absicherung dieser Infrastrukturen werden im Normalfall Firewalls eingesetzt, die nicht erwünschte Netzpakete ausfiltern können. Dazu müssen Firewallssysteme den Netzverkehr auf mehreren Protokollschichten (typisch sind Netz- und Transportschicht) analysieren, die verwendeten Protokolle identifizieren und letztendlich entscheiden, ob die Daten weitergeleitet oder verworfen werden. Aktuelle Trends in

der Entwicklung von Netzprotokollen zeigen allerdings auf, dass immer häufiger so genannte Overlaystrukturen eingesetzt werden, und somit auf der Anwendungsschicht mehrere Protokolle ineinander verschachtelt werden. Beispielhaft seien hier Web 2.0-Technologien erwähnt, wie sie etwa im Google-Maps-Dienst zur Anwendung kommen. Angriffe auf dieser Ebene können mit existierenden Firewall-Technologien noch nicht erkannt werden.

Ziel des Projekts PADIOFIRE ist es, ein neuartiges Firewallsystem zu entwickeln, welches eine semantische Analyse von mehrfach geschachtelten Anwendungsprotokollen am Beispiel von Web 2.0-Diensten durchführen kann. Die Ergebnisse der Analyse stellen die Grundlage für die Entscheidung dar, ob zugehörige Datenströme weitergeleitet oder verworfen werden. Konkret ist es geplant, ein Intrusion-Detection-System (IDS) als Basis zu nutzen, welches auf die Erkennung von bestimmten Strukturen, vorrangig Angriffen, im Netzverkehr spezialisiert ist und somit gut geeignet für die Anwendungs- und Protokollerkennung ist. Da aktuelle IDS-Ansätze nicht auf die semantische Analyse von Overlaystrukturen spezialisiert sind, welche für eine genaue Analyse auf Anwendungsebene nötig ist, soll eine neuartige Regelsprache entwickelt werden, welche mehrfach geschachtelte Anwendungsprotokolle detailliert analysiert. Die semantische Analyse von Anwendungsdaten ist sehr aufwändig, daher sind architektonische Optimierungen geplant. Zum einen spielt die verteilte Analyse auf mehreren Prozessorkernen eine essentielle Rolle und zum anderen ist die Entwicklung einer losen Kopplung von Analyse und Firewall geplant.

vmFIRE (*Firewalling in virtuellen Maschinen*) - Teilvorhaben Entwicklung eines Redirektormoduls und Analyse von Migrationsstrategien und – verfahren bei Virtuellen Maschinen

BMBF-Verbundvorhaben

(gemeinsames Projekt mit der *genua (Gesellschaft für Netzwerk- und UNIX-Administration)* mbH Kirchheim)

01.07.2012 - 30.06.2014

Radoslaw Cwalinski, René Rietz, Hartmut König

Firewallsysteme, die innerhalb der einzelnen Virtuellen Maschinen eingerichtet werden, bieten ein erhöhtes Angriffsprofil, da diese anfälliger für Angriffe sind (das Kompromittieren eines virtuellen Servers bedeutet gleichzeitig die der darin laufenden Firewall), die Systemleistung der virtuellen Umgebung erheblich beeinträchtigt wird und eine zusätzliche manuelle Konfiguration innerhalb jeder virtuellen Maschine erforderlich ist. Durch die Einrichtung einer logisch separierten Firewall-Umgebung kann ein Schutzniveau vergleichbar mit dem herkömmlicher, physikalisch getrennter Firewalls erreicht werden. In diesem Projekt sollen verschiedene Virtualisierungsmechanismen, z. B. die vollständige Virtualisierung, Paravirtualisierung und Betriebssystemvirtualisierung, hinsichtlich der Schnittstellen für ein effizientes Monitoring der virtuellen Netzwerke untersucht und geeignete Sensoren dafür entwickelt werden. Die Migration von laufenden virtuellen Maschinen auf andere Hostsysteme stellt dabei eine besondere Herausforderung für ein lückenloses Monitoring dar. Hierfür muss die Konfiguration der Firewalls (a) über verschiedene Virtualisierungstechnologien hinweg und (b) auf die veränderten Umgebungsbedingungen Bezug nehmend dynamisch angepasst und ebenfalls migriert werden. Da der virtuelle Netzverkehr jederzeit die Übertragungsrate eines physikalischen Netzes bei Weitem übersteigen kann, können

die Firewall-Sensoren innerhalb der Virtualisierungsumgebungen einen Engpass darstellen. Deshalb ist die Performanz der mit den Sensoren verbundenen Firewallsysteme von hoher Bedeutung. Da Firewallsysteme Echtzeitanforderungen besitzen, sollen in diesem Projekt erstmalig die Auswirkungen beim Einsatz auf virtuellen Maschinen untersucht werden.

Studie zur Sicherung der IT-Sicherheit von Prozessrechensystemen

Vattenfall Europe Generation AG

01.08.2012 – 28.02.2013

Andreas Paul, Franka Schuster

Im Rahmen der Studie wird die Reduzierung der Risiken für Nichtverfügbarkeiten von Prozessrechensystemen in Folge von IT-Bedrohungen an einem Kraftwerksstandort der Vattenfall Europe Generation AG untersucht. Dazu gehören die Analyse der vorhandenen bzw. gelebten Sicherheitstechnologien und –verfahren, ein Abgleich mit dem aktuellen Stand von Wissenschaft und Technik bezüglich der IT-Sicherheit von prozessnahen Steuer- und Regelsystemen in kritischen Infrastrukturen, die Bewertung der aktuellen Bedrohungslage (u. a. entsprechend der BSI-Anforderungen) sowie die Entwicklung konzeptioneller Maßnahmen zur Erhaltung bzw. Verbesserung der IT-Sicherheit auf Grundlage der Bestandsanalyse und unter Berücksichtigung der besonderen Anforderungen / Randbedingungen an Steuer- und Regelsysteme in Kraftwerken.

P2P Intrusion Detection

Michael Vogel

Der Einsatz von Multiagenten- und Peer-to-Peer-Technologien wird in den letzten Jahren auch im Bereich des Intrusion Detection intensiv untersucht. Diese Technologien bieten eine Vielzahl neuer, interessanter Möglichkeiten für die Überwachung verteilter Systeme und Anwendungen. Erste Ansätze liegen bereits vor. Die großen Vorteile für das Intrusion Detection liegen in der Dezentralisierung, der Robustheit, der Kooperation, der Selbstorganisation und der Skalierbarkeit. Solche Systeme erlauben es, erforderliche Überwachungsstrukturen dynamisch und flexibel auf den Einsatzfall zugeschnitten zu generieren. Sie werden mittelfristig die relativ starren und dedizierten Systeme, wie sie heutzutage im Einsatz sind, ablösen. Das wird langfristig auch Kosten reduzieren, da die Systeme kooperativ genutzt zu werden können. Die Nutzung von Multiagenten- und P2P-Technologien im Intrusion Detection wirft ein breites Spektrum neuer Probleme auf bzw. verschärft einige der bereits im Kontext der verteilten IDS sichtbar gewordenen Fragestellungen. Schwerpunkt des Projekts ist die Untersuchung von ausgewählten Aspekten der Gestaltung flexibler verteilter Intrusion Detection Systeme. Dabei wird sich auf die Durchführung effizienter und sicherer Analysen in solchen Systemen konzentriert, die bisher kaum betrachtet wurden. Es sollen Verfahren untersucht werden, die in Überlastsituationen Analysen automatisch auf andere Komponenten verlagern, ohne Ursprung und Bedeutung der Analysedaten preiszugeben. Dabei zugleich eine effiziente und korrekte Analyse sichern.

UML-basierte Entwicklung von Kommunikationsprotokollen

Prabhu Shankar Kaliappan, Hartmut König

Die Unified Modeling Language UML hat eine breite Anwendung zur Modellierung und Entwicklung von komplexen Softwaresystemen gefunden. Bei der Entwicklung von Kommunikationsprotokollen wird UML bisher weniger genutzt. In diesem Projekt soll eine Methodik entwickelt werden, wie UML ausgehend von den Erfahrungen mit den klassischen formalen Beschreibungstechniken, wie SDL, Lotos, u. a., zur Entwicklung und Validierung von Kommunikationsprotokollen genutzt werden kann.

BTU International Graduate School, ZUSYS (*Dependable Hardware / Software Systems*)

Stefanie Judith Opitz, Mario Pink, Hartmut König

Postoperative patients as well as people with chronic diseases need a special, often permanent monitoring. Nowadays, such a monitoring can usually only be provided for inpatients. An equally, reliable ambulatory monitoring is required because a hospitalization is very cost-intensive and also often inconvenient for the patients themselves. Collaborative electronic systems using today's mobile networks may be a solution to this problem enabling a mobile patient monitoring and thus avoiding a hospitalization. This will increase the compliance of the patients which is often important for their convalescence.

Accordingly, the goal of the proposed research theme is the design of a dependable patient monitoring systems based on the use of mobile collaborative services. Important design aspects are the convenience for patients and medical personnel on the one hand, and the security and dependability of the patient monitoring on the other hand. Hereby the handling of network outages is of special interest. Depending on the kind of failure different reactions are conceivable. The most desirable one is the use of a different, available network. Ideally, the hand-over to another network would be completely transparent for the medical applications. To evaluate this possibility, the *uBeeMe* platform currently being developed in the group of Prof. König will be used. For the case that the switch to another network is not possible or a reliable network connection cannot be guaranteed, methods using caching schemes in conjunction with rudimentary medical intelligence inside the mobile devices will be investigated. If even these methods do not help, nonetheless there has to be a solution for the monitoring of the patients. Therefore, it will be analyzed by what means the system can detect these exceptional circumstances and what kind of indication should be given to patients and physicians to realize an immediate alternative (non-mobile) monitoring. The monitoring systems will be implemented as prototype and evaluated in experiments.

Veröffentlichungen

1. König, H.; Gäbler, J.; Klauck, R.; Pink, M.; Sprejz, M.: uBeeMe - A Platform for Mobile Collaborative Applications. *Praxis der Informationsverarbeitung und Kommunikation (PIK)* 36(1):43 (2013)
2. Gaebler, J.; Koenig, H.: Enhancing Group Communication Systems with Mobility Support. In: *Proceedings of the 19th IEEE International Conference on Networks (ICON 2013)*, Singapore, December 2013.
3. Gäbler, J.; Klauck, R.; Pink, M.; König, H.: uBeeMe - a Platform to Enable Mobile Collaborative Applications. In: *Proceedings of the 9th International Conference on Collaborative Computing: Networking, Applications and Worksharing (Collaborate-Com 2013)*, Austin, Texas, USA, October, 2013, pp. 188-196.
4. Gaebler, J.; Koenig, H.: Moversight: A Group Communication Protocol for Mobile Collaborative Applications. In: *Proceedings of the 6th Joint IFIP Wireless and Mobile Networking Conference (WMNC 2013)*, Dubai, United Arab Emirates, 23 - 25th April 2013.
5. Gaebler, J.; Koenig, H.: Moversight: An Approach to Support Mobility in Collaborative Applications. Poster presented as part of the 10th Annual Conference on Wireless On-Demand Network Systems and Services (WONS 2013), Banff, Alberta, Canada, March 2013.
6. Kirsche, M.; Hartwig, J.: A 6LoWPAN Model for OMNeT++. In: *Proceedings of the 6th International OMNeT++ Workshop, co-located with the 6th International ICST Conference on Simulation Tools and Techniques (SIMUTools 2013)*, Cannes, France, March 2013. - Presented Poster
7. Kirsche, M. Simulating the Internet of Things in a Hybrid Way. In: *Proceedings of the Networked Systems (NetSys) 2013, PhD Forum*.
8. Klauck, R.; Kirsche, M.: Enhanced DNS Message Compression - Optimizing mDNS/DNS-SD for the Use in 6LoWPANs. In: *Proceedings of the 9th IEEE International Workshop on Sensor Networks and Systems for Pervasive Computing 2013 (PerSeNS 2013)*, co-located with the 11th IEEE Conference on Pervasive Computing and Communication (PerCom 2013), San Diego, California, USA, March, 2013.
9. Klauck, R.; Kirsche, M. Combining Mobile XMPP Entities and Cloud Services for Collaborative Post-Disaster Management in Hybrid Network Environments. *Mobile Networks and Applications - The Journal of SPECIAL ISSUES on Mobility of Systems, Users, Data and Computing* Vol. 18 (2), pp. 253 – 270, 2013.
10. Mehner, S.; Klauck, R.; König, H.: Location-Independent Fall Detection with Smartphone. In: *Proceedings of the 6th International Conference on Pervasive Technologies Related to Assistive Environments (PETRA '13)*, Rhodes Island, Greece, 29 – 31 May 2013, ACM, New York, NY, USA, 2013, Article 11 , 8 pages, DOI=10.1145/2504335.2504346.
11. Paul, A., Schuster, F., König H.: Towards the Protection of Industrial Control Systems - Conclusions of a Vulnerability Analysis of Profinet IO. In: *Proceedings of the 10th*

International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2013, Berlin, Germany, July 18-19, 2013, pp. 160-176.

12. Schuster, F., Paul, A., König, H.: Towards Learning Normality for Anomaly Detection in Industrial Control Networks. In: Proceedings of the 7th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security (AIMS 2013), Barcelona, Spain, June 2013, LNCS 7943, Springer, pp. 61-72, 2013.
 13. Pink, M.; Sprejz, M.; König, H.: A Coordinated Group Decision for Vertical Handovers in Heterogeneous Wireless Networks. International Conference on Mobile Wireless Middleware, Operating Systems, and Applications (MOBILWARE), Bologna, Italy, November 2013, pp. 130-137.
-

Vorträge

- 12.03.2013: *Michael Kirsche*:
Simulating the Internet of Things in a Hybrid Way. Networked Systems (NetSys) 2013, PhD Forum.
- 19.03.2013: *Jan Gäbler*:
Moversight: An Approach to Support Mobility in Collaborative Applications. 10th Annual Conference on Wireless On-Demand Network Systems and Services (WONS 2013), Banff, Alberta, Kanada, 2013.
- 22.03.2013: *Ronny Klauck*:
Enhanced DNS Message Compression - Optimizing mDNS/DNS-SD for the Use in 6LoWPANs. 9th IEEE International Workshop on Sensor Networks and Systems for Pervasive Computing 2013 (PerSeNS 2013), co-located with the 11th IEEE Conference on Pervasive Computing and Communication (PerCom 2013), San Diego, California, USA, 2013.
- 23.04.2013: *Jan Gäbler*:
Moversight: A Group Communication Protocol for Mobile Collaborative Applications. 6th Joint IFIP Wireless and Mobile Networking Conference (WMNC 2013), Dubai, 2013.
- 29.05.2013: *Stefan Mehner*:
Location-Independent Fall Detection with Smartphone. 6th International Conference on Pervasive Technologies Related to Assistive Environments (PETRA '13), Rhodes Island, Greece, 2013.
- 27.06.2013: *Franka Schuster*:
Towards Learning Normality for Anomaly Detection in Industrial Control Networks. 7th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security (AIMS 2013), Barcelona, Spain, 2013.
- 19.07.2013: *Andreas Paul*:
Towards the Protection of Industrial Control Systems - Conclusions of a Vulnerability Analysis of Profinet IO. 10th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2013, Berlin, 2013.
- 22.10.2013: *Jan Gäbler*:
uBeeMe - a Platform to Enable Mobile Collaborative Applications. 9th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2013), Austin, Texas, USA, 2013.

- 11.11.2013: *Mario Pink:*
A Coordinated Group Decision for Vertical Handovers in Heterogeneous
Wireless Networks. International Conference on Mobile Wireless Middleware,
Operating Systems, and Applications (MOBILWARE), Bologna, Italy
- 13.12.2013: *Jan Gäbler:*
Enhancing Group Communication Systems with Mobility Support. 19th IEEE
International Conference on Networks (ICON 2013), Singapore, 2013.
-

Dissertationen, Diplom-, Bachelor- und Studienarbeiten

Dissertationen

keine

Diplomarbeiten

Brandt, Stefan: *Entwicklung eines Netzwerk-Discovery-Algorithmus für heterogene Netze.* Januar 2013.

Buchheim, Daniel: *HTTP-normalisierende Proxies.* August 2013.

Masterarbeiten

Schneider, Grit: *Entwurf und Simulation eines Dienstes zur Erkennung von Netzpartitionierung in einer mobilen P2P-Gruppenkommunikationssitzung.* Februar 2013.

Schnurbusch, Matti: *Entwurf und Implementierung eines flexiblen IEEE 802.15.4 Simulationsmodells für OMNeT++.* Juli 2013

Bachelorarbeiten

Stahl, Alexander: *Selbstoptimierende Netzauswahl für Handover in heterogenen drahtlosen Netzen.* Februar 2013.

Schwalbe, Christoph: *Untersuchung der Portierbarkeit von TLS auf Contiki OS.* November 2013.

Mitarbeit in Gremien

König, Hartmut:

- *BTU Cottbus*
 - Mitglied im Fakultätsrat der Fakultät Mathematik, Naturwissenschaften und Informatik
 - Vorsitzender der Kommission *Forschung und wissenschaftlicher Nachwuchs*
 - stellv. Mitglied im Senat der BTU Cottbus

- Mitgliedschaften
 - Mitglied IFIP TC6/WG6.1 "Architecture and Protocols for Computer Networks"
 - Mitglied im erweiterten Leitungsgremium der GI-Fachgruppe "Kommunikation und verteilte Systeme (KuVS)"

Vogel, Michael:

- *BTU Cottbus*
 - Mitglied im Prüfungsausschuss Informatik

Rechnerausstattung

Die Rechnerausstattung des Lehrstuhls ist 2013 im Wesentlichen unverändert geblieben.

Auszeichnungen

Sonstiges

Prof. König weilte von April – August 2013 zu einem Forschungsaufenthalt am Department of Network Software, TELECOM & Management SudParis in Evry in der Gruppe von Prof. A. Cavalli.
