Jahresbericht 2012

Inhaltsverzeichnis

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:	Katrin Willhöft	
Akademische Mitarbeiter:	M.Sc. Michael Kirsche Dipl.-Inf. Michael Vogel	
Projektmitarbeiter:	B.Sc. Radoslaw Cwalinski Dipl.-Inf. Jan Gäbler Dipl.-Inf. Ronny Klauck M.Sc. Andreas Paul M.Sc. René Rietz M.Sc. Franka Schuster M.Sc. Michael Sprejz	seit 01.06.2012 seit 01.05.2012
Technischer Mitarbeiter:	Dipl.-Inf. Joachim Paschke	
Doktoranden:	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
- Handovertechniken
- 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 2011/2012

- Vorlesung "Rechnernetze und Kommunikationssysteme I"
- Praktikum "Rechnernetze und Kommunikationssysteme"
- Vorlesung "IT-Sicherheit"
- Praktikum "Mobile kollaborative Anwendungen"
- Oberseminar

Sommersemester 2012

- Vorlesung "Rechnernetze und Kommunikationssysteme II"
- Fortgeschrittenenpraktikum "Rechnernetze und Kommunikationssysteme"
- Vorlesung "Protocol Engineering"
- Vorlesung "Betriebssysteme und Rechnernetze für Ingenieure"
- Projektseminar "Netzwerksimulation"
- Proseminar "Trends in Kommunikationstechnologien"
- Oberseminar

Wintersemester 2012/2013

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

Radoslaw Cwalinski, Jan Gäbler, Ronny Klauck, Andreas Paul, Franka Schuster, Michael Sprejz

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 Aquisition*) – 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

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, welche unerwünschte Netzwerkpakete ausfiltern können. Dazu müssen Firewallsysteme den Netzwerkverkehr auf mehreren Protokollschichten (typisch sind Netzwerk- und Transportschicht) analysieren, die verwendeten Protokolle identifizieren und letztendlich entscheiden, ob die Daten weitergeleitet oder verworfen

werden. Aktuelle Trends in der Entwicklung von Netzwerkprotokollen zeigen allerdings auf, dass immer häufiger sogenannte Overla-ystrukturen eingesetzt werden, und somit auf der Anwendungsschicht mehrere Protokolle inei-nander 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 Netzwerkverkehr 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

René Rietz

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 separier-ten 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 Umgebungs-bedingungen 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 Virtualisierungs-umgebungen 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.

Evaluierung der Verfügbarkeit von Funkübertragungsstrecken in MANETs

Forschungsunterauftrag für das Fraunhofer Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) Wachtberg

01.05.2012 - 30.11.2012

Radoslaw Cwalinski

Ziel des Projekts ist die Evaluierung von verteilten Sensoren zur Erfassung von Dienstgüteeigenschaften in mobilen Ad-hoc-Netzen. Die Verfügbarkeit von Diensten und der zugrunde liegenden Netzinfrastruktur stellt ein wesentliches Schutzziel in taktischen mobilen Ad-Hoc-Netzen (sog. MANETs) dar. Dieses Ziel kann häufig wegen stark beschränkter Ressourcen – z. B. Rechenleistung, Übertragungs- und Batteriekapazitäten – sowie wegen der Anfälligkeit für Denial-of-Service-Angriffe nicht erreicht werden. Da viele Faktoren in nicht-trivialer Weise die Verfügbarkeit des Netzes und der Dienste beeinflussen, ist es auf den ersten Blick meist nicht offensichtlich, aus welchem Grund eine Verringerung der Verfügbarkeit vorliegt. In MANETs sind daher zuverlässige Messverfahren notwendig, die bei der Bestimmung der Verfügbarkeit von Funkübertragungsstrecken helfen. Um der Ressourcenlimitierung von MANETs gerecht zu werden, wurde ein auf passiver Beobachtung basierender Ansatz für eine Verfügbarkeits-Sensorik am FKIE entworfen und prototypisch implementiert und evaluiert.

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, Hartmut König

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 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 patent 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. Carle, G.; Debar, H.; Dressler, F.; König, H.: Network Attack Detection and Defense Early Warning Systems - Challenges and Perspectives (Dagstuhl Seminar 12061). Dagstuhl Reports 2(2): 1 - 20 (2012).
2. Kaliappan, P.S.; König, H.: On the Formalization of UML Activities for Component-Based Protocol Design Specification, 38th International Conference on Current Trends in Theory and Practice of Computer Science, Špindlerv Mlýn, Czech Republic, LNCS 7147, pp. 479 - 491. Springer, Prague (2012).
3. Kirsche, M; Klauck, R.: Unify to Bridge Gaps: Bringing XMPP into the Internet of Things. In Proceedings of the Work in Progress Session of the 10th IEEE Conference on Pervasive Computing and Communication (PerCom 2012), Lugano, Switzerland, March 2012.
4. Klauck, R.; Kirsche, M.: XMPP to the Rescue: Enhancing Post Disaster Management and Joint Task Force Work. In Proceedings of the 2nd International Workshop on Pervasive Networks for Emergency Management (PerNEM) in Cooperation with the 10th IEEE Conference on Pervasive Computing and Communication (PerCom 2012), Lugano, Switzerland, March 2012.
5. Klauck, R.; Kirsche, M.: Bonjour Contiki: A Case Study of a DNS-Based Discovery Service for the Internet of Things. In Proceedings of the 11th International IEEE Conference on Ad-Hoc Networks and Wireless (ADHOC-NOW 2012), ser. Lecture Notes in Computer Science (LNCS), X.-Y. Li, S. Papavassiliou, and S. Ruehrup, Eds., vol. 7363. Springer, July 2012, pp. 317 – 330.
6. Klauck, R.; Kirsche, M.: Combining Mobile XMPP Entities and Cloud Services for Collaborative Post-Disaster Management in Hybrid Network Environments. In Mobile Networks and Applications - The Journal of SPECIAL ISSUES on Mobility of Systems, Users, Data and Computing. Springer, Online Publication August 2012. DOI: 10.1007/s11036-012-0391-1.
7. Klauck, R.; Kirsche, M.: Chatty Things - Making the Internet of Things Readily Usable for the Masses with XMPP. In Proceedings of the 8th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2012), Pittsburgh, Pennsylvania, USA, October, 2012.
8. Koall, S.; Klauck, R.: Dualisierung graphischer Benutzeroberflächen: Portierung einer GUI vom Desktop auf Smartphone, AV Akademikerverlag, 100 Seiten, April 2012, ISBN 978-3639391268.
9. König, H.: Network Attack Detection and Defense. Praxis der Informationsverarbeitung und Kommunikation (PIK) 35(1):1 (2012).
10. König, H.: Protocol Engineering. Springer-Verlag, 2012, 525 Seiten, ISBN 978-3-642-29144-9.
11. Liu, F; Koenig, H.: Puzzle - an efficient, compression independent video encryption algorithm. Multimedia Tools and Applications, 10.1007/s11042-012-1185-y, 2012.
12. Paul, A.: Verwundbarkeitsanalyse des Industrial-Ethernet Protokolls Profinet IO. In Patrick Stewin und Collin Mulliner, editor, Proceedings of the Seventh GI SIG SIDAR

Graduate Workshop on Reactive Security (SPRING). Technical Report SR-2012-01, page 10. GI FG SIDAR, Berlin, Juli 2012.

13. Paul, A.; Schuster, F.; König, H.: Profinet IO Vulnerability Assessment and Attack Derivation. In Preproceedings of the Seventh International Conference on Critical Information Infrastructures Security, pp. 127 - 130, Lillehammer, Norway, September 2012.
14. Pink, M.; Pietsch, T. Koenig, H.: Towards a seamless mobility solution for the real world: Hand-over decision. International Symposium on Wireless Communication Systems 2012, pp. 651 – 655, August 2012, Paris, France.
15. Pink, M.; Pietsch, T. Koenig, H.: An adaptive Handover decision algorithm for heterogeneous wireless networks, Mobilware 2012, November 2012, Berlin, Germany.
16. Schuster, F.: Intrusion Detection for Automation Technology. In Patrick Stewin und Collin Mulliner, editors, Proceedings of the Seventh GI SIG SIDAR Graduate Workshop on Reactive Security (SPRING). Technical Report SR-2012-01, page 14. GI FG SIDAR, Berlin, Juli 2012.
17. Schuster, F.; Paul, A.; König, H.: A Distributed Intrusion Detection System for Industrial Automation Networks. In Proceedings of the 17th International Conference on Emerging Technologies & Factory Automation, Krakau, Polen, September 2012.
18. Vogel, M.; Rietz, R.; Schmerl, S.: Automated Generation of Precise Signatures. In: Praxis der Informationsverarbeitung und Kommunikation (PIK), 35 (2012) 1, pp. 40 – 45, DE GRUYTER/SAUR, Berlin/Munich, 2012.

Vorträge

23.01.2012:
Prabhu S. Kaliappan: On the Formalization of UML Activities for Component-Based Protocol Design Specifications, 38th International Conference on Current Trends in Theory and Practice of Computer Science, Špindlerv Mlýn, Czech Republic, 2012.

07.02.2012:
Franka Schuster: Protecting Critical Infrastructures, Dagstuhl Seminar on Network Attack Detection and Defense Early Warning Systems – Challenges and Perspectives, Wadern, 2012.

09.02.2012:
René Rietz: Intrusion Detection for the Web 2.0. Dagstuhl Seminar on "Net-work Detection and Defense, Early Warning Systems - Challenges and Perspectives", Wadern, 2012.

Michael Vogel: A Dynamically Adapting Distributed Multi Agent IDS. Dagstuhl Seminar on "Network Detection and Defense, Early Warning Systems - Challenges and Perspectives", Wadern, 2012.

20.03.2012:
Michael Kirsche: "Unify to Bridge Gaps: Bringing XMPP into the Internet of Things", Work in Progress Session of the 10th IEEE Conference on Pervasive Computing and Communication (PerCom 2012), Lugano, Switzerland.

05.07.2012:
Andreas Paul: Verwundbarkeitsanalyse des Industrial-Ethernet Protokolls Profinet IO, Seventh GI SIG SIDAR Graduate Workshop on Reactive Securi-ty (SPRING), 2012.

Franka Schuster: Intrusion Detection for Automation Technology, Seventh GI SIG SIDAR Graduate Workshop on Reactive Security (SPRING), 2012.

30.08.2012:
Mario Pink: Towards a seamless mobility Solution for the real World: Handover Decision, ISWCS 2012, Paris, France, 2012.

17.09.2012:
Andreas Paul: Profinet IO Vulnerability Assessment and Attack Derivation, Seventh International Conference on Critical Information Infrastructures Security, 2012.

19.09.2012:
Franka Schuster: A Distributed Intrusion Detection System for Industrial Automation Networks, 17th International Conference on Emerging Technologies & Factory Automation, 2012.

26.09.2012:
Hartmut König, René Rietz: PADIOFIRE: Firewalls für das Web 2.0, Bochum, Projektseminar zum Forschungsprogramm IT-Sicherheit, 2012.

15.10.2012:
Ronny Klauck: Chatty Things - Making the Internet of Things Readily Usable for the Masses with XMPP, CollaborateCom 2012, Pittsburgh, Pennsylvania, USA, 2012.

13.11.2012:
Mario Pink: An adaptive Handover decision algorithm for heterogeneous wireless networks, Mobilware 2012, Berlin.

Dissertationen, Diplom-, Bachelor- und Studienarbeiten

Dissertationen

keine

Diplomarbeiten

Cwalinski, Radoslaw:	*Schnittstellenvirtualisierung für die opportunistische Nutzung von 802.11 Netzen.* Mai 2012.
Bude, Robert:	*Integration eines Self-Repairing-Mechanismus in das Gruppenkommunikationsprotokoll GCP.* Juli 2012.

Masterarbeiten

Sprejz, Michael:	*Entwicklung und Evaluation eines energieeffizienten verteilten Handover-Entscheidungsalgorithmus für kollaborative Anwendungen in heterogenen drahtlosen Netzen.* April 2012.
Brachmann, Martina:	*Security for CoAP-based End-to-End Scenarios in the Internet of Things.* November 2012.

Bachelorarbeiten

Kremmer, Roman:	*Porting Contiki for Waspmote Sensor Nodes.* Januar 2012.
Haeseler, Christian:	*Übertragung von Geoinformationen zwischen den Teilnehmern eines XMPP-Netzes.* April 2012.
Hoffmann, Paul:	*Entwicklung eines Testbeds zur Untersuchung von XMPP für Smarthome-Szenarios.* April 2012.
Mehner, Stefan:	*Portierung eines Algorithmus zur Sturzerkennung auf ein Smartphone. Oktober 2012.*
Brase, Sebastian:	*Contiki Unterstützung für die Sensorik der Waspmote-Plattform.* Oktober 2012.

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)"

- *Mitglied im Programmkomitee*

Vogel, Michael:

- *BTU Cottbus*
  - Mitglied im Prüfungsausschuss Informatik

Rechnerausstattung

Die Rechnerausstattung des Lehrstuhls ist 2012 im Wesentlichen unverändert geblieben.

Auszeichnungen

Stefanie J. Opitz, Fachklasse ZUSYS:
1. Preis "Emergency Medical Data Transmission: Assisting Medical Care with Dynamic Data Priorization", Posterausstellung am 2. Forschungstag (07.06.2012) der BTU Cottbus "Wissen schafft Freu(n)de – Forschung macht Spaß" im Rahmen der Energiewoche.

Link: http://www.tu-cottbus.de/btu/de/gradschool/igs/aktuelles.html

Sonstiges

Dagstuhl Seminar 12061: Network Attack Detection and Defense - Early Warning Systems – Challenges and Perspectives

Die Erkennung und Abwehr von Attacken im Internet war Gegenstand des auf Initiative des Lehrstuhls Rechnernetze und Kommunikationssysteme zusammen mit Prof. Georg Carle (TU München), Prof. Hervé Debar (Telecom ParisSud), und Dr. Jelena Mirkovic (USC Marina del Rey) veranstalteten Seminars Network Attack Detection and Defense, das vom 5. – 10. Februar 2012 in Schloss Dagstuhl bei Wadern (Saarland) stattfand. An ihm nahmen mehr als 30 Spezialisten aus den USA, Frankreich, Großbritannien, Österreich, Schweden, Norwegen, Luxemburg, den Niederlanden und Deutschland teil, um aktuelle Entwicklungen bei der Aufdeckung und Abwehr von Internetangriffen zu diskutieren. Schwerpunkt des Seminars waren Anforderungen an die Gestaltung von Frühwarnsystemen zur Malwareerkennung und Abwehr von Attacken. Die Ergebnisse des Seminars sind in einem Dagstuhl Report zusammengefasst, der unter http://drops.dagstuhl.de/opus/volltexte/2012/3476/ einsehbar ist. Der Report wurde unter Mitarbeit von Franka Schuster erstellt.