Lehrstuhl Rechnernetze und Kommunikationssysteme

Personelle Zusammensetzung

Leitung:
Prof. Dr.-Ing. Hartmut König

Sekretariat:
Katrin Willhöft

Akademische Mitarbeiter:

B.Sc. Radoslaw Cwalinski	Projektmitarbeiter, bis 31.05.2011
M.Sc. Matthias Dreißig	Projektmitarbeiter, bis 31.05.2011
Dipl.-Inf. Jan Gäbler	Projektmitarbeiter
M.Sc. Michael Kirsche	
Dipl.-Inf. Ronny Klauck	Projektmitarbeiter
Dipl. Inf. Ralf Kopsch	Projektmitarbeiter, bis 15.11.2011
Dipl.-Inf. Maik Krüger	Projektmitarbeiter, bis 31.05.2011
Dr.-Ing. Liu, Fuwen	Projektmitarbeiter, bis 31.05.2011
M.Sc. Andreas Paul	Projektmitarbeiter, seit 15.09.2011
Dipl.-Inf. Mario Pink	Projektmitarbeiter, bis 31.05.2011
Dipl.-Inf. Daniel Rakel	Projektmitarbeiter, bis 31.03.2011
M.Sc. René Rietz	Projektmitarbeiter
Dipl.-Inf. Sebastian Schmerl	Projektmitarbeiter, bis 31.01.2011
Dipl.-Inf. Sebastian Schöpke	Projektmitarbeiter, bis 15.11.2011
M.Sc. Franka Schuster	Projektmitarbeiterin, seit 15.10.2011
Dipl.-Inf. Michael Vogel	

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
- Mobile Mehrteilnehmer-Videokonferenzen
- Wireless Personal Networks (IEEE 802.15)
- Plattformen für die Unterstützung mobiler kollaborativer Anwendungen

(2) Protocol Engineering

- UML basierte Protokollentwicklung

(3) Sicherheit in Rechnernetzen

- Peer-to-Peer Intrusion Detection
- Signaturableitung und -validation
- Gruppenschlüsselmanagement für verteilte mobile Anwendungen

Lehrveranstaltungen

Wintersemester 2010/2011:

- Vorlesung „Rechnernetze und Kommunikationssysteme I“
- Praktikum „Rechnernetze und Kommunikationssysteme“
- Vorlesung „Protocol Engineering“
- Seminar „Mobile kollaborative Anwendungen“
- Oberseminar

Sommersemester 2011:

- Vorlesung „Rechnernetze und Kommunikationssysteme II“
- Fortgeschrittenenpraktikum „Rechnernetze und Kommunikationssysteme“
- Vorlesung „Innovative Netztechnologien“
- Praktikum „Mobile kollaborative Anwendungen für Sensornetze“
- Proseminar „Trends in Kommunikationstechnologien“
- Oberseminar

Wintersemester 2011/2012:

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

Forschungsprojekte

Plattform für mobile kollaborative Anwendungen
BMBF-Programm ForMaT "Forschung für den Markt im Team" Phase II
(gemeinsames Projekt mit dem Lehrstuhl *ABWL und Besondere des Marketing und des Innovationsmanagement*)

01.06.2009 – 31.5.2011

Daniel Baier, Radoslaw Cwalinski, Matthias Dreißig, Jan Gäbler, Michael Kirsche, Ronny Klauck, Hartmut König, Ralf Kopsch, Mike Krüger, Fuwen Liu, Mario Pink, Daniel Rakel, René Rietz, Sebastian Schöpke, Sebastian Selka

Das InnoLab „Plattform für mobile kollaborative Anwendungen“ beschäftigt sich mit der Erforschung und Entwicklung von Bausteinen für eine kollaborative und mobile Gestaltung und Nutzung von Anwendungen. Entwickelt wird die Plattform uBeeMe zur Unterstützung von mobilen kollaborativen Anwendungen in den Bereichen Smart Home, Online Gaming, Audio/Video-Kollaboration, Mobile Health Care oder Facility Management, die gegenwärtig im Rahmen des BMBF ForMaT Programms an der BTU Cottbus entwickelt wird. Es handelt sich um eine Software-Plattform, die Basisfunktionen für kollaborative Anwendungen in Form von Diensten auf heterogenen Systemen (Desktop PCs, Note- und Netbooks, Smartphones) und Laufzeitumgebungen (z.B. Windows Desktop und Windows Mobile) bereitstellt. uBeeMe kommt dabei durch den Einsatz von Peer-2-Peer- (P2P-) Ansätzen ohne eine komplexe Server-Infrastruktur aus und unterstützt dadurch insbesondere Anwendungen in mobilen Ad-hoc Szenarien. Charakteristische Merkmale der uBeeMe-Plattform sind:

- Offenheit und Erweiterbarkeit
  Die Plattform kann durch Plugins, zum Beispiel von Drittanbietern, flexibel erweitert und dadurch an individuelle Anforderungen angepasst werden.
- Unterstützung dynamischer Gruppenkommunikation
  Neben Punkt-zu-Punkt-Kommunikation unterstützt die Plattform Gruppenkommunikation und den damit verbundenen Aufbau und die Verwaltung von geschlossenen Nutzergruppen mit sich ändernden Teilnehmerzahlen und Gruppenmitgliedschaften.
- Kollaborationsunterstützung
  Die Plattform stellt Dienste zur Unterstützung verschiedener Kollaborationsformen bereit (bspw. Audio, Video, Chat, u.v.a.), welche die Kooperation von Kommunikationspartnern und Gruppen fördern.
- Transparente Netznutzung
  Die Plattform ermöglicht durch adaptive Handover-Funktionalitäten die transparente und gleichzeitige Nutzung kollaborativer Anwendungen über verschiedene Netze (Fest- und Mobilfunknetze).
- Vertrauliche und sichere Kommunikation
  Die Plattform sichert bei Bedarf eine vertrauliche und verschlüsselte Kommunikation sowohl für Punkt-zu-Punkt-Verbindungen als auch für Gruppenkommunikationsanwendungen.

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

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.

Überwachung von Netzinfrastruktur mittels Intrusion Detection Overlays
Förderprogramm „Forschungs- und Innovationsförderung zur Steigerung der Innovationskraft an Brandenburger Hochschulen“

01.06.2011 – 31.12.2011

Prabhu S. Kaliappan, Ralf Kopsch, Sebastian Schöpke

Attacken im Internet werden heute häufig hochgradig verteilt ausgeführt, indem tausende fremd kontrollierte Rechnersysteme, die zu so genannten Botnetzen zusammengefasst wurden, genutzt werden, um Rechner gezielt anzugreifen bzw. durch Denial of Service-Angriffe in ihrer Funktion zu hindern oder zu blockieren. Die Nutzung verteilter Ansätze im Intrusion Detection, z. B. durch die Nutzung von Multiagenten- oder Peer-to-Peer-Technologien, stellt eine logische Konsequenz zur Abwehr solcher Angriffe dar. Bisherige derartige Ansätze nutzen bisher nur die Möglichkeiten der Kooperation zur Verteilung von Analyseresultaten, z. B. Angriffswarnungen. Ziel des Forschungsvorhabens ist die Entwicklung von verteilten Intrusion Detection (ID) Systemen, die unter Nutzung der Peer-to-Peer-Technologie als ID-Overlay für den Schutz von unterschiedlichen Netzinfrastrukturen (Intranets, Unternehmensnetze, Internet Service Provider Netzen, Campus-Netzen u. a.) eingesetzt werden können und eine gesamtheitliche Überwachung solcher Netze ermöglichen. Dabei sollen Verfahren entwickelt werden, die in Überlastsituationen Analysen automatisch auf andere Analyseeinheiten (ID-Agenten) verlagern, ohne Ursprung und Bedeutung der Analysedaten preiszugeben. Diese Problematik, einschließlich der Korrelation von Teilergebnissen der verteilten Analyse in einem ID-Overlay, bildet die wissenschaftliche Herausforderung dieses Vorhabens.

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 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 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.

Intrusion Detection/Signatur Analyse

Sebastian Schmerl, Hartmut König

Intrusion-Detection-Systeme sind ein wichtiges Instrument für den Schutz informationstechnischer Ressourcen. Ihnen kommt als Grundlage reaktiver Sicherheitsmechanismen eine wachsen-

de Bedeutung zu. In Ergänzung präventiver Sicherheitsmechanismen ermöglichen sie eine automatische Erkennung und ggf. auch eine Abwehr von IT-Sicherheitsverletzungen. Das Forschungsvorhaben konzentriert sich auf den Bereich der Signaturanalyse. Die Wirksamkeit der Signaturanalyse hängt entscheidend von der Genauigkeit der verwendeten Signaturen ab. Ungenaue Signaturen schränken die Erkennungsmächtigkeit der Intrusion-Detection-Systeme stark ein und führen u. a. zu Fehlalarmen. Die Ursachen der Erkennungsunsicherheit sind nur teilweise in qualitativen Einschränkungen der Audit-Funktionen zu suchen. Die Ableitung der Signaturen aus gegebenen Exploits ist häufig der entscheidende Schwachpunkt. Ihre Ableitung erfolgt zumeist empirisch. Ziel des Projekts ist die Entwicklung von Verfahren für eine systematische Ableitung von Signaturen aus Exploits. Damit sollen vor allem der empirische Anteil bei der Ableitung der Signaturen als auch der Entwicklungsaufwand reduziert werden. Für die Validierung der Signaturen werden zur Verifikation von Signaturen, u. a. mittels des Model Checkers SPIN, und zum Test von Signaturen entwickelt.

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

Brachmann, M.; Garcia-Morchon, O.; Kirsche, M.: Security for Practical CoAP Applications: Issues and Solution Approaches. In 10. GI/ITG KuVS Fachgespräch Sensornetze, September, 2011.

Gaebler, J.; Klauck, R.; Kopsch, R.; Liu, F.; Pink, M.; Schoepke, S; Koenig, H.: Mobile kollaborative Apps. In Smart Mobile Apps - Mit Business-Apps ins Zeitalter mobiler Geschäftsprozesse. Springer, Xpert.press Serie, Kapitel 29, Seiten 447 - 463, 2012, ISBN 978-3-642-22259-7.

Gaebler, J.; Klauck, R.; Schöpke, S.; König, H.: Lemon Tree – Flexible Deichüberwachung mit XMPP und Cloud-Diensten. In 8. GI/KuVS-Fachgespräch Ortsbezogene Anwendungen und Dienste, S. 137 – 148, München, September, 2011.

Kaliappan, P.S.: *Uncertainty, Protocol Behavior Prediction Through Chaos Theory?* IEEE International Conference on Uncertainty Reasoning and Knowledge Engineering, Bali, Indonesia, Volume 1, pp. 20 - 23. IEEE, Bali (2011).

Kaliappan, P.S.; König, H.: An Approach to Synchronize UML-based Design Components for Model-Driven Protocol Development, IEEE 34th Software Engineering Workshop, Ireland, June 2011.

Klauck, R.: Integration von P2PSIP in eine kollaborative Anwendung: Am Beispiel des P2P-Videokonferenzsystems BRAVIS, VDM Verlag Dr. Müller, 136 Seiten, Juli 2011, ISBN 978-3639367140.

Klauck, R.; Kirsche, M., Gaebler, J., Schoepke, S.: Mobile XMPP and Cloud Service Collaboration: An Alliance for Flexible Disaster Management. In Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2011), Orlando, USA, October, 2011.

Kirsche, M.; Dreissig, M.; Kopsch, R.; Gaebler, J.; Klauck, R.; Pink, M.; Liu, F.; Koenig, H.: uBeeMe – Eine Plattform zur Unterstützung mobiler kollaborativer Anwendungen. In PIK - Praxis der Informationsverarbeitung und Kommunikation. Vol. 34, Issue 1, pp. 11 - 22, DOI: 10.1515/PIKO.2011.003, January - March 2011.

Liu, F.; Koenig, H.: Cryptanalysis of a SIP Authentication Scheme. IFIP International Conference on Communications and Multimedia Security 2011, LNCS 7025, pp. 134 - 143, October 19th - 21st, 2011, Ghent, Belgium.

Liu, F.; Koenig, H.: A Simple Balanced Password-Authenticated Key Agreement Protocol. IEEE TrustCom 2011, November 16th - 18th, Changsha, China.

Vorträge

20.06.2011: Prabhu Shankar Kaliappan: An Approach to Synchronize UML-based Design Components for Model-Driven Protocol Development. IEEE 34th Software Engineering Workshop, Ireland, 2011.

04.08.2011: Prabhu Shankar Kaliappan: Uncertainty, Protocol Behavior Prediction Through Chaos Theory? IEEE International Conference on Uncertainty Reasoning and Knowledge Engineering, Bali, Indonesia, 2011.

09.09.2011: Sebastian Schöpke: Lemon Tree – Flexible Deichüberwachung mit XMPP und Cloud-Diensten. 8. GI/KuVS-Fachgespräch Ortsbezogene Anwendungen und Dienste, München, 2011.

16.09.2011: Martina Brachmann: Security for Practical CoAP Applications: Issues and Solution Approaches. 10. GI/ITG KuVS Fachgespräch Sensornetze, Paderborn, 2011.

17.10.2011: Ronny Klauck: Mobile XMPP and Cloud Service Collaboration: An Alliance for Flexible Disaster Management. 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2011), Orlando, USA, 2011.

21.10.2011: Fuwen Liu: Cryptanalysis of a SIP Authentication Scheme. IFIP International Conference on Communications and Multimedia Security 2011, Ghent, Belgium, 2011.

18.11.2011: Fuwen Liu: A Simple Balanced Password-Authenticated Key Agreement Protocol. IEEE TrustCom 2011, Changsha, China, 2011.

Bachelorarbeiten

Meier, Denis: Vergleich und Evaluation verschiedener IEEE 802.15.4 Simulationsmodelle. März 2011

Hennig, Marc: Machbarkeitsstudie für eine Brücke und eine Abhöranwendung für IEEE 802.15.4 Netzwerke. März 2011

Lösche, Jürgen: Entwicklung einer P2P-Komponente für ein Multi-Agenten-basiertes IDS. April 2011

Koall, Sebastian: Dualisierung grafischer Benutzeroberflächen: Portierung einer GUI vom Desktop auf Smartphone. September 2011

Böhm, Sebastian: Erweiterung der Einsatzgebiete von IEEE 802.15.4 Sniffern und Netzwerkmonitoren. Oktober 2011

Rühr, Marcel: Auffinden und Gruppieren von Teilnehmern in einem XMPP-Netz. November 2011

Krumholz, Andreas: Evaluierung der Contiki Netzwerk-Stacks für den Einsatz in drahtlosen Gesundheitsanwendungen. November 2011

Masterarbeiten

Pietsch, Thomas: Entwicklung und Evaluation eines energieeffizienten Handover-Entscheidungsalgorithmus für drahtlose heterogene Netzwerke. Juni 2011

Paul, Andreas: Anwendungserkennung durch Verkehrsanalyse mittels Netz-basierter Intrusion Detection Systeme. August 2011

Schuster, Franka: Entwicklung des Aufgabenplaners für ein verteiltes, agentenbasiertes Intrusion-Detection-System. Oktober 2011

Gäbler, Silvio: Entwurf und Auswertung von Diensten zum Aufteilen und Vereinigen mobiler Gruppenkommunikationssitzungen. Oktober 2011

Urban, Mandy: Exploration von Netzwerkdomänen durch Verkehrsanalyse. November 2011

Diplomarbeiten

Schöpke, Sebastian: Entwurf und Entwicklung einer adaptiven Benutzerlokalisierung für Ad-hoc- und Infrastruktur-Umgebungen. Februar 2011

Berger, Andreas: Parallelisierung von NIDS am Beispiel von Snort. April 2011

Mrose, Martin: Sensornetzwerke in Simulation und Praxis: Vergleich eines IEEE 802.15.4 Simulationsmodells mit einem realen Sensornetz. Mai 2011

Dissertationen

Schmerl, Sebastian: Ansätze zur systematischen Ableitung von Signaturen – Methoden im Entwicklungsprozess einer Signatur. April 2011

Mitarbeit in Gremien

König, Hartmut:

- *BTU Cottbus*
  - Mitglied des Fakultätsrat der Fakultät Mathematik, Naturwissenschaften und Informatik
  - Vorsitzender der Kommission *Forschung und wiss. 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 in Programmkomitees*
  - KIVS 2011 Kiel

Vogel, Michael:

- *BTU Cottbus*
  - Mitglied im Prüfungsausschuss Informatik

Rechnerausstattung

Auszeichnungen

Sonstiges