Jahresbericht 2010

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:	M.Sc. Matthias Dreißig Dipl.-Inf. Jan Gäbler Dipl.-Inf. Ronny Klauck

	Dipl.-Inf. Maik Krüger Dipl.-Ing. Liu, Fuwen Dipl.-Inf. Mario Pink Dipl.-Inf. Daniel Rakel M.Sc. René Rietz Dipl.-Inf. Sebastian Schmerl	bis 31.03.2010
Technischer Mitarbeiter:	Dipl.-Inf. Joachim Paschke	
Doktoranden:	M.Sc. Prabhu Shankar Kaliappan M.Sc. Stefanie Judith Opitz	

Zum Inhaltsverzeichnis

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

(2) Protocol Engineering

- UML basierte Protokollentwicklung

(3) Sicherheit in Rechnernetzen

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

Zum Inhaltsverzeichnis

Lehrveranstaltungen

Wintersemester 2009/2010:

- Vorlesung "Rechnernetze und Kommunikationssysteme I"
- Praktikum "Rechnernetze und Kommunikationssysteme"
- Vorlesung "Innovative Netztechnologien"

- Projektseminar "Netzwerk-Simulation"
- Oberseminar

Sommersemester 2010:

- Vorlesung "Rechnernetze und Kommunikationssysteme II"
- Fortgeschrittenenpraktikum "Rechnernetze und Kommunikationssysteme"
- Vorlesung "IT-Sicherheit"
- Vorlesung "Betriebssysteme und Rechnernetze für Ingenieure"
- Proseminar "Trends in Kommunikationstechnologien"
- Oberseminar

Wintersemester 2010/2011:

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

Zum Inhaltsverzeichnis

Forschungsprojekte

Plattform für mobile kollaborative Anwendungen

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

01.06.2009 - 31.05.2011

Daniel Baier, Matthias Dreißig, Jan Gäbler, Michael Kirsche, Ronny Klauck, Hartmut König, Ralf Kopsch, Fuwen Liu, Mario Pink, Daniel Rakel, René Rietz 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.

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 wachsende 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 werden Verfahren untersucht, 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. Grundlage ist die Entwicklung einer formalen Semantik für UML.

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

Stefanie Judith Opitz, 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.

Projektbezogener Personenaustausch mit Norwegen

(Norwegian University of Science and Technology (NTNU) Trondheim, Department of Telematics, Prof. Peter Herrmann)
DAAD-Programm

01.01.2009 – 31.12.2010

Prabhu Shankar Kaliappan, Hartmut König, Sebastian Schmerl, Michael Vogel

The goal of the cooperation between the research groups in Cottbus and Trondheim is to apply model-based collaborative system engineering, the focus of the Trondheim group, to a systematic development of P2P intrusion detection systems, the research area of the Cottbus group. Based on the system engineering approach SPACE of the Trondheim group a methodology for the model-based development of intrusion detection systems shall be developed and proved for its applicability. Model based engineering enables the fast design, generation, and validation of intrusion detection systems and facilitate the design and adaptation of needed protocols and system components. Moreover, the models can be analyzed for security gaps and hardened by adding security mechanisms. In order to prove the feasibility of the methodology a prototype system shall be designed, automatically implemented, and validated. To achieve these goals, a number of tasks have to be performed:

- The collaborative system engineering approach SPACE which currently is dedicated mainly to the design of networked services and its toolset Arctis shall be extended to enable the automated creation and security analysis of communication protocols, in particular P2P protocols.
- A number of protocols have to be designed supporting the interaction of agents in P2P intrusion detection systems and the corresponding Arctis-model building blocks must be developed.
- The example system has to be specified using the model building blocks, checked for design errors by the Arctis inspectors and model checking tools. To cover vulnerabilities and threads of the modeled system, a security analysis has to be performed. The resulting system model must be synthesized and the appropriate code generated by means of the Arctis tools.
- The generated implementation shall be thoroughly validated and improvements for

both the intrusion detection protocols and the SPACE-engineering process shall be identified.

Zum Inhaltsverzeichnis

Veröffentlichungen

1. Gunawan, L A., Vogel, M., Kraemer, F.A., Schmerl, S., Slåtten, V., Herrmann, P., König, H.: Modeling a Distributed Intrusion Detection System using Collaborative Building blocks. In: 3rd IEEE International Workshop UML and Formal Methods, Shanghai, China, Nov 16, 2010.
2. Kaliappan, P. S.; König, H.; Schmerl, S.: Model-Driven Protocol Design Based on Component Oriented Modeling. In: J. S. Dong and H. Zhu (eds.) 12th International Conference on Formal Engineering Methods (ICFEM 2010), Shanghai. LNCS 6447, pp. 613 - 629. Springer, Heidelberg, 2010.
3. Kirsche, M.: IEEE 802.15.4 Performance Analysis. In Wehrle, K.; Günes, M.; Gross, J. (Eds.): Modeling and Tools for Network Simulation. Springer, chap. 13.2, pp. 317 - 325, ISBN: 978-3-642-12330-6, 2010.
4. Liu, F.; Koenig, H.: A Survey of Video Encryption Algorithms. Computers&Security, Volume 29, Issue 1, February 2010, pp. 3 - 15, ISSN: 0167-4048.
5. Rietz, R., Schmerl, S., Vogel, M., König, H.: Iterative präzisionsbewertende Signaturgenerierung. In: Freiling, F. C. (ed.) Sicherheit 2010, Lecture Notes in Informatics 170, GI, 2010.
6. Schmerl, S.; Vogel, M.; Rietz, R; Koenig, H.: Explorative Visualization of Log Data to Support Forensic Analysis and Signature Development. In: Proceedings of the Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, SADFE 2010, Oakland, CA, USA, ISBN: 978-0-7695-4052-8, May 2010.
7. Vogel, M.: Topologie-angepasste Overlays für Peer-to-Peer Intrusion Detection. In: Sebastian Schmerl, Simon Hunke (Eds.) Proceedings of the Fifth GI SIG SIDAR Graduate Workshop on Reactive Security (SPRING). Technical Report SR-2010-01, page 13. GI FG SIDAR, Bonn, Juli 2010.

Zum Inhaltsverzeichnis

Vorträge

11.03.2010:
Vogel, M.: Peer-To-Peer Intrusion Detection Overlays, ZAB Brandenburg - Transfertag "Sicherheitswitrtschaft trifft Wissenschaft", Königs-Wusterhausen.

07.07.2010:
Vogel, M.: Topologieadaptierte P2P-Informationsoverlays, 5. GI FG SIDAR Graduierten-Workshop Reaktive Sicherheit – SPRING, Bonn.

06.10.2010:
Rietz, R.: Iterative Signature Generation", ISSE/GI Sicherheit2010, SIG SIDAR, Berlin.

06.10.2010:
Vogel, M.: Peer-to-Peer Intrusion Detection", ISSE/GI Sicherheit2010 SIG SIDAR, Berlin.

19.11.2010:
Kaliappan, P.S.: Model-Driven Protocol Design Based on Component Oriented Modeling, 12th International Conference on Formal Engineering Methods (ICFEM 2010), Shanghai, China.

Zum Inhaltsverzeichnis

Dissertationen, Diplom-, Bachelor- und Studienarbeiten

Dissertationen

Diplomarbeiten

Puder, Sebastian:	*Verifikation von EDL-Signaturen*. Juni 2010.

Masterarbeiten

Schwarzer, Susanne:	*Vertrauens- und Kreditierungsmechanismen für verteilte Intrusion-Detection-Systeme*. April 2010.
Roloff, Fabian:	*Analyseverteilungs- und –verlagerungsmechanismen für ein signaturbasiertes IDS*. Juni 2010.

Bachelorarbeiten

Brachmann, Martina:	*Integration von realen Anwendungen in Simulationsumgebungen*. Januar 2010.
Link, Nicole:	*Aufzeichnung von geschlossenen P2P-Videokonferenzen*. März 2010.
Schneider, Grit:	*Synchronisation von UML-Sequenz- und Aktivitätsdiagrammen*. September 2010.

Kantor, Thomas: *Design und Evaluierung von grafischen Benutzeroberflächen für mobile und stationäre Systeme*. November 2010.

Zum Inhaltsverzeichnis

Mitarbeit in Gremien

König, Hartmut:

- *BTU Cottbus*
  - Mitglied im Fakultätsrat der Fakultät Mathematik, Naturwissenschaften und Informatik
  - Mitglied 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 SDL-Forum
- *Mitglied im Programmkomitee*
  - TestCom 2010, Natal, Brasilien
  - DAIS 2010, Amsterdam, Niederlande
  - SAM 2010, Oslo, Norwegen

Schmerl, Sebastian:

- *Mitgliedschaften*
  - Steering Komitee SIG SIDAR (Security - Intrusion Detection and Response)
- Mitglied in Programmkomitees
  - DIMVA 2010 (Publicity Chair)
    SIG SIDAR Conference on Detection of Intrusions and Malware & Vulnerability Assessment
  - Spring 2010 (Program Chair)
    SIDAR Graduierten-Workshop über Reaktive Sicherheit
  - Sicherheit 2010 – Spezial Session: Reaktive IT-Sicherheit (Co-Chair)
    Reaktive IT-Sicherheit: Erkennung und Beherrschung von IT-Sicherheitsvorfällen
  - DIMVA 2010 Bonn
    SIG SIDAR Conference on Detection of Intrusions and Malware & Vulnerability Assessment
  - LCN Sick-Workshop 2010 Denver, USA
    Security in Communication Networks
  - Sicherheit 2010 Berlin
    Sicherheit, Schutz und Zuverlässigkeit

Vogel, Michael:

- *BTU Cottbus*

- Mitglied im Prüfungsausschuss Informatik

Zum Inhaltsverzeichnis

Rechnerausstatung

Die Rechnerausstattung des Lehrstuhls wurde im Rahmen der Sonderzuweisung der Universitätsleitung durch das ForMaT-Projekt in 2009 wesentlich erweitert und modernisiert. Sie ist in 2010 im Wesentlichen unverändert geblieben

Zum Inhaltsverzeichnis

Auszeichnungen

Zum Inhaltsverzeichnis

Sonstiges

CeBIT 2010: Eine Plattform zur Unterstützung mobiler kollaborativer Anwendungen

Vorgestellt 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) für verschiedene Lauf¬zeit¬um¬gebungen (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
- Unterstützung dynamischer Gruppenkommunikation
- Kollaborationsunterstützung
- Transparente Netznutzung
- Vertrauliche und sichere Kommunikation

Zum Inhaltsverzeichnis

letzte Änderung: mvogel, 22.03.2013 16:34 Uhr