Jahresbericht 2014/15

Inhaltsverzeichnis

Personelle Zusammensetzung

Lehrstuhlleiter:	Prof. Dr.-Ing. habil. Hartmut König	
Adresse:	Brandenburgische Technische Universität Cottbus-Senftenberg 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.Sebastian Böhm	seit 12/2014
	M.Sc. Michael Kirsche	bis 02/2015
	M.Sc. Andreas Paul	
	Dipl.-Inf. Michael Vogel	bis 01/2014
Projektmitarbeiter:	M.Sc. Radoslaw Cwalinski	seit 01/2015
	Dipl.-Inf. Jan Gäbler	
	M.Sc. Michael Kirsche	seit 02/2015
	Dipl.-Inf. Ronny Klauck	bis 10/2014
	M.Sc. René Rietz	
	M.Sc. Franka Schuster	
Technischer Mitarbeiter:	Dipl.-Inf. Joachim Paschke	
Doktoranden:	M.Sc. Radoslaw Cwalinski	bis 12/2014
	M.Sc. Prabhu Shankar Kaliappan	
	M.Sc. Stefanie Judith Opitz	bis 04/2015
	Dipl.-Inf. Mario Pink	
	Dipl.-Inf. Michael Vogel	seit 01/2014

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 2013/2014

- Vorlesung „Grundlagen der Rechnernetze“
- Praktikum „Grundlagen der Rechnernetze“
- Vorlesung „Protocol Engineering“
- Projektseminar „Netzwerksimulation“
- Oberseminar

Sommersemester 2014

- Vorlesung „Internet - Funktionsweise, Protokolle, Anwendungen“
- Vorlesung „Betriebssysteme und Rechnernetze für Ingenieure“
- Fortgeschrittenenpraktikum „Rechnernetze und Kommunikationssysteme“
- Praktikum/Seminar „Internet der Dinge“
- Praktikum „Protocol Engineering“
- Proseminar „Trends in Kommunikationstechnologien“
- Oberseminar

Wintersemester 2014/2015

- Vorlesung „Grundlagen der Rechnernetze“
- Praktikum „Grundlagen der Rechnernetze“
- Vorlesung "IT-Sicherheit"
- Projektseminar „Netzsimulation“
- Oberseminar

Sommersemester 2015

- Vorlesung „Internet - Funktionsweise, Protokolle, Anwendungen“
- Vorlesung "Protocol Engineering"
- Proseminar „Trends in Kommunikationstechnologien“
- Praktikum „Protocol Engineering“
- Oberseminar

Wintersemester 2014/2015

- Vorlesung „Grundlagen der Rechnernetze“
- Praktikum „Grundlagen der Rechnernetze“
- Vorlesung "IT-Sicherheit"
- Projektseminar „Netzwerksimulation“
- Oberseminar

Forschungsprojekte

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 - 30.11.2014

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.

Entwicklung eines Monitoring- und Sicherheitssystems für komplexe DECT-Anlagen (MOSDAN)

BMWi ZIM-Kooperationsprojekt
(gemeinsames Projekt mit der COMPLUS GmbH Calau)

01.06.2014 – 31.05.2016

Jan Gäbler

Das Projekt MOSDAN hat die Entwicklung eines modular aufgebauten Monitoring- und Sicherheitssystems für komplexe DECT-Anlagen einschließlich der Entwicklung und

Implementierung einer Referenzbake, zum Inhalt. Es verfolgt das Ziel, das Management verteilter Anlagen für die mobile Unternehmenskommunikation zu verbessern, eine einfache standortübergreifende Verwaltung von Komponenten der mobilen Unternehmenskommunikation zu ermöglichen und in Verbindung mit einer neuartigen Referenzbake die funktechnische Versorgung in sicherheitskritischen Bereichen eines Unternehmens zu überwachen und zu sichern. MOSDAN ist ein modulares System und besteht aus den Komponenten Umbrella Management, Monitoring Appliance und der Referenzbake. Mit dem Einsatz von MOSDAN werden kundenseitig sowohl wesentliche Zugewinne bezüglich der Sicherheit aller DECT-bezogenen Kommunikationsprozesse als auch signifikante Rationalisierungseffekte bei Wartung und Instandhaltung von DECT-Kommunikationssystemen erreicht. MOSDAN kann in bestehende DECT-Anlagen und in Neuanlagen integriert werden.

Im Fokus des Projekts stehen DECT-basierte Telefonanlagen (*Digital Enhanced Cordless Telecommunications - Standard*), die bei der unternehmensinternen Mobilkommunikation in Deutschland und auch europaweit den höchsten Verbreitungsgrad aufweisen. Der Einsatz des neuartigen Monitoring- und Sicherheitssystems ist vorgesehen in:

- diversen Handels-/Verkaufsunternehmen mit einer Vielzahl von Standorten
- Krankenhäusern
- Kreuzschifffahrtsflotten (z.B. AIDA-Cruises)
- Industrieanlagen.

INDI (*Intelligente Intrusion-Detection-Systeme für Industrienetze*) – Teilvorhaben: Monitoring von Industrienetzen mit Hilfe automatisierter Topologieexploration und selbstlernender Anomalieerkennung für standardisierte Industrieprotokolle

BMBF-Verbundprojekt
(gemeinsames Projekt mit der Vattenfall Europe Generation AG, der Georg-August-Universität Göttingen und der *genua (Gesellschaft für Netzwerk- und UNIX-Administration) mbH* Kirchheim)

01.11.2014 - 31.10.2017

Andreas Paul, René Rietz, Franka Schuster, Hartmut König

Das Projekt INDI hat den intelligenten Schutz von Industrienetzen in kritischen Infrastrukturen zum Ziel. Projektinhalt ist die Entwicklung einer neuartigen Technologie zur Analyse, Erkennung und Eindämmung von Cyberangriffen in heterogenen Industrienetzen mit Echtzeitanforderungen. Der Anspruch der Verbundpartner ist es dabei, durch einen hohen Grad an Selbstjustierung eine alltagstaugliche, kosteneffiziente, benutzerfreundliche und an die Komplexität der Infrastruktur gut skalierbare Sicherheitslösung zu schaffen, die unabhängig von den konkreten industriellen Prozessen der Industrienetze eingesetzt werden kann.

Im Rahmen des Projekts sollen Sicherheitstechniken entwickelt werden, die erstmals eine robuste Erkennung von Angriffen in komplexen Industrienetzen mit zum Teil unbekannten Protokollen ermöglichen. Hierzu wird die angestrebte Sicherheitslösung in die Industrienetze des Betreibers eingebracht und analysiert in einer Phase der Selbstjustierung den dortigen Netzverkehr mit Techniken des maschinellen Lernens. Ziel dieser automatischen Analyse ist

es, zum einen Regeln und Modelle für den Normalbetrieb abzuleiten und zum anderen unbekannte Protokolle zu beobachten und nachzubilden. Eine Verfeinerung der Regel- und Modellableitung wird zusätzlich durch eine automatische Schwachstellenanalyse ermöglicht.

SICIA (*Security Indicators for Critical Infrastructure Analysis*) – Teilvorhaben: Entwurf und Implementierung eines Prozesses zur quantitativen Bewertung der IT-Sicherheit von industriellen Steuerungssystemen

BMBF-Verbundprojekt
(gemeinsames Projekt mit der Vattenfall Europe Generation AG und RWE Deutschland AG)

01.11.2014 - 31.10.2017

Andreas Paul, René Rietz, Franka Schuster, Hartmut König

Moderne Informationstechnik wird zur Überwachung und Steuerung von Kraftwerken und Versorgungsnetzen genutzt. Allerdings mangelt es an Methoden zur Messung der IT-Sicherheit in diesen Netzen, die die technische Zuverlässigkeit von Komponenten und Systemen angemessen beurteilen. Ziel des Projekts SICIA (*Security Indicators for Critical Infrastructure Analysis*) ist es, neue Lösungsansätze mithilfe von belastbaren Sicherheitsindikatoren und Softwarewerkzeugen zu entwickeln.

Im Projekt wird ein Verfahren entwickelt, mit dessen Hilfe Betreiber kritischer Infrastrukturen den Ist-Zustand der IT-Sicherheit in ihren Anlagen ermitteln können. Diese Art von Bewertung wird bereits in vielen branchenspezifischen Richtlinien als Voraussetzung für eine kontinuierliche Verbesserung der sicherheitsrelevanten IT-Prozesse verlangt. Ein konkretes Vorgehen, das es erlaubt, auch komplexe Infrastrukturen bis auf Geräteebene differenziert zu bewerten, ist jedoch bisher nicht verfügbar. Im Gegensatz zu existierenden Bewertungsverfahren wird bei der im Projekt SICIA entwickelten Analyse auf die Betrachtung schwer bestimmbarer, kaum quantifizierbarer Bedrohungen verzichtet. Die entwickelten Sicherheitsindikatoren verdichten vor allem technische Parameter in Zahlenwerte, um die tatsächliche IT-Sicherheit für Betreiber sichtbar zu machen.

Der Vergleich der ermittelten Sicherheitsindikatoren auf System- und Geräteebene erlaubt im Anschluss die Erkennung von Schwachstellen und eine Priorisierung von Verbesserungsmaßnahmen in komplexen Infrastrukturen. Zur Unterstützung der Beurteilung potenzieller Verbesserungsmaßnahmen wird ein Werkzeug entwickelt. Dieses erlaubt eine automatisierte Ermittlung von Kenngrößen, deren Verdichtung sowie eine Simulation der Auswirkungen potenzieller Verbesserungsmaßnahmen. Besonders effektive Maßnahmen werden so sichtbar und können vom Betreiber ausgewählt werden.

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 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

2014

1. Dacier, M.; Kargl, F.; König, H.; Valdes, A.: Network Attack Detection and Defense: Securing Industrial Control Systems for Critical Infrastructures. Report from Dagstuhl Seminar 14292, 13. – 16. Juli 2014, S. 62 – 79, Dagstuhl reports ; vol. 4, issue 7.
2. Kargl, F.; Heijden, R. W. van der; König, H.; Valdes, A.; Dacier, M. C.: Insights on the Security and Dependability of Industrial Control Systems. IEEE Security & Privacy, S. 75 – 78, Band/Jahrgang: 12, Ausgabe/Heft: 6, ISSN: 1540-7993.
3. Gäbler, J.; König, H.; Enhancing Group Communication Systems with Mobility Support. In: Proceedings of the 19th IEEE International Conference on Networks (ICON 2013), Singapore, Dec. 2013, pp. 342 - 347, ISBN: 978-1-4799-2085-3, 2014.
4. Kirsche, M.; Schnurbusch, M.: A New IEEE 802.15.4 Simulation Model for OMNeT++ / INET. In: Proceedings of the 1st International OMNeT++ Community Summit (OMNeT 2014), Hamburg, Germany, Sept. 2014.
5. Liu, F.; König, H.: Puzzle - an efficient, compression independent video encryption algorithm. Multimedia tools and applications, S. 715 – 735, Band/Jahrgang: 73, Ausgabe/Heft: 2, ISSN: 1573-7721.
6. Opitz, S. J.; Todtenberg, N.; König, H.: Mobile bandwidth prediction in the context of emergency medical service. In: Proceedings of the 7th International Conference on PErvasive Technologies Related to Assistive Environments (PETRA '14). ACM, New York, NY, USA, 2014, Article 49, 7 pages. DOI=10.1145/2674396.2674411.
7. Rietz, R.; Vogel, M.; Schuster, F.; König, H.: Parallelization of Network Intrusion Detection Systems under Attack Conditions. In: Proceedings of the 11th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2014, Egham, UK, July 2014, LNCS 8550, Springer, pp. 172 – 191, 2014.
8. Schuster, D.; Grubitzsch, P.; Renzel, D.; Koren, I.; Klauck, R.; Kirsche, M.: Global-scale Federated Access to Smart Objects Using XMPP. In: Proceedings of the IEEE International Conference on Internet of Things (iThings 2014), Taipei, Taiwan, September, 2014.

2015

1. Böhm, S.; Kirsche, M.: Looking into Hardware-in-the-Loop Coupling of OMNeT++ and RoSeNet. In: Proceedings of the 2nd International OMNeT++ Community Summit (OMNeT 2015), Zurich, Switzerland, September, 2015.
2. Förster, A.; Minkenberg, C.; Herrera, G. R.; Kirsche, M.: Proceedings of the 2nd International OMNeT++ Community Summit (OMNeT 2015), Zurich, Switzerland on September 3-4, 2015.
3. Gäbler, J.; König, H.: Moversight: a group communication protocol for mobile scenarios. In: Telecommunication Systems: Modeling, Analysis, Design and Management, Springer, June 2015. DOI10.1007/s11235-015-0062-1.

4. Gaebler, J.; Koenig, H.: Distributed Latency Estimation Using Global Knowledge for Mobile Collaborative Applications. In: Proceedings of the 11th International Wireless Communications & Mobile Computing Conference (IWCMC 2015), Dubrovnik, Croatia, 24-27th Aug. 2015, pp. 474 – 479.
5. Kirsche, M.; Kremmer, R.: uIP Support for the Network Simulation Cradle. In: Proceedings of the 2nd International OMNeT++ Community Summit (OMNeT 2015), Zurich, Switzerland, September, 2015.
6. Schuster, F., Paul, A., Rietz, R., König, H.: Potentials of Using One-class SVM for Detecting Protocol-specific Anomalies in Industrial Networks. In: Proceedings of the 2015 IEEE Symposium on Computational Intelligence in Cyber Security (IEEE CICS 2015), IEEE Press, New York, 2015, pp. 83 - 90.

Vorträge

29.05.2014: *Stefanie Judith Opitz*:
Mobile bandwidth prediction in the context of emergency medical service. PETRA '14, Rhodos, Greece.

11.07.2014: *René Rietz*:
Parallelization of Network Intrusion Detection Systems under Attack Conditions. DIMVA 2014, Egham, UK.

02.09.2014: *Michael Kirsche*:
A New IEEE 802.15.4 Simulation Model for OMNeT++ / INET. OMNeT 2014, Hamburg, Germany.

24.08.2015: *Jan Gäbler*:
Distributed Latency Estimation Using Global Knowledge for Mobile Collaborative Applications. IWCMC 2015, Dubrovnik, Croatia

03.09.2015: *Michael Kirsche*:
uIP Support for the Network Simulation Cradle. OMNeT 2015, Zürich, Switzerland, 2015.

08.12.2015: *Franka Schuster*:
Potentials of Using One-class SVM for Detecting Protocol-specific Anomalies in Industrial Networks. IEEE CICS 2015, Cape Town, South Africa, 2015.

Diplom-, Bachelor- und Studienarbeiten

Diplomarbeiten

Matthies, Falko:	*Untersuchung zur Ersetzung der protokollabhängigen Erkennung von Netzdiensten durch mDNS/DNS-SD.* Juli 2014.

Masterarbeiten

Stubbe, Felix:	*Entwurf und Umsetzung eines verteilten Topologie-Wartungsdienstes für das mobile Gruppenkommunikationsprotokoll Moversight.* Juni 2014.
Meier, Denis:	*Dual-Radio Unterstützung für Contiki am Beispiel der Waspmote Plattform.* August 2014.
Böhm, Sebastian:	IEEE 802.15.4 Sensornetz-Emulation am Praxisbeispiel RoSeNet. Dezember 2014.
Haeseler, Christian:	*Erstellung einer automatisierten Testumgebung zur Evaluierung der Integration von intelligenten Dingen in das Internet*. März 2015.
Radebach, Patrick:	*Entwurf und Umsetzung eines effizienten Aggregationsverfahrens für den „Chatty-Things“ – Ansatz*. März 2015.
Mehner, Stefan:	*Hühnerwasser goes smart! Ein Konzept für ein nachhaltiges Umweltmonitoringsystem*. Juli 2015.

Bachelorarbeiten

Brilka, Dennis:	*Entwurf und Umsetzung einer autonomen, kooperativen Lego-Nxt-Gruppe zur Gebäudeüberwachung*. April 2014.
Krieg, Björn:	*Stochastische Analyse von Funksignalen zur Handover Initiierung.* April 2014.
Noack, Robert:	*Walle - eine virtuelle Testumgebung für die realistische Simulation von Benutzern innerhalb einer Moversight basierten, mobilen, kollaborativen Anwendung*. Oktober 2014.
Hannusch, Robert:	*Analyse von Netzwerkdaten mittels Kommunikationsgraphen*. Mai 2015.

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

Dagstuhl-Seminar 14292

„Network Attack Detection and Defense - Securing Industrial Control Systems for Critical Infrastructures”

Der Lehrstuhl Rechnernetze und Kommunikationssysteme (Prof. König) hat gemeinsam mit Prof. Dr. F. Kargl (Universität Ulm), Prof. A. Valdes (Universität von Illinois - Urbana Champaign) und Dr. Marc Dacier (Qatar Computing Research Institute Doha) das Dagstuhl-Seminar 14292 zum Schutz industrieller kritischer Infrastrukturen (http://www.dagstuhl.de/de/programm/kalender/semhp/?semnr=14292) organisiert. An ihm nahmen mehr als 30 Spezialisten aus den USA, Frankreich, Großbritannien, den Niederlanden, Luxembourg, Österreich, Schweden und Deutschland teil, um aktuelle Entwicklungen und neue Ansätze für die Sicherung von industriellen Steuerungssystemen zu diskutieren. In Vorträgen und Arbeitsgruppen wurden neuste Forschungsergebnisse vorgestellt und Ansätze zur Verhinderung von Angriffen auf industrielle Steuerungssysteme aus dem Internet diskutiert. Daraus wurden Schwerpunkte für zukünftige Forschungen abgeleitet. Die Ergebnisse des Seminars sind in den Dagstuhl-Proceedings (http://www.dagstuhl.de/de/programm/kalender/semhp/?semnr=14292) zusammengefasst.

Netsys 2015

Der Lehrstuhl hat vom 9. bis 12. März 2015 die Internationale Fachtagung NetSys 2015 (**www.netsys2015.com**) organisiert, die auf dem Zentralcampus der BTU stattfand. Die Tagung stand unter der Leitung von Prof. Dr.-Ing. Hartmut König und Prof. Dr. rer. nat. Peter Langendörfer (Leibniz-Institut für innovative Mikroelektronik Frankfurt (Oder)). Die Netsys (*Conference on Networked Systems*) ist eine internationale Konferenz zu den Themenbereichen Rechnernetze, drahtlose und drahtgebundene Kommunikation sowie vernetzte und verteilte Systeme im Allgemeinen. Sie ist aus der deutschen Fachtagung KiVS (Kommunikation in Verteilten Systemen) hervorgegangen, die zum ersten Mal 1979 in Berlin durchgeführt wurde und seitdem in einem zweijährigen Rhythmus stattfand. Die Konferenz wird von der Fachgruppe "Kommunikation und Verteilte Systeme" (KuVS) der Gesellschaft für Informatik (GI) ausgerichtet. Die IEEE hatte das technische Co-Sponsorship übernommen. Die akzeptierten 22 Beiträge der Konferenz sowie die Vorträge der zwei anschließenden Workshops wurden in der IEEE Xplore-Bibliothek veröffentlicht.

An der Konferenz nahmen über 150 Wissenschaftler aus 10 Ländern teil. Es vier eingeladene Vorträge. Frau Prof. Klara Nahrstedt von der University of Illinois at Urbana-Champaign (USA) berichtete über erste Erfahrungen mit der neuen Technologie des Software-Defined Networking bei Echtzeit-Anwendungen. Dr. Marc Dacier vom Qatar Computing Research Institute (Katar) hat in einem sehr anschaulichen Vortrag Defizite des zentralen Internet-Routingprotokolls BGP diskutiert, die für Cyber-Angriffe auf die grundlegende Infrastruktur des Internets ausgenutzt werden können.

Gastland der NetSys 2015 war Polen. Führende Wissenschaftler gaben einen Überblick über die Netzforschung in unserem Nachbarland und berichteten über aktuelle Forschungsprojekte und Kooperationen. Dr. Norbert Meier vom Supercomputing and Networking Center Poznan stellte das polnische Hochleistungsrechnernetz und die Möglichkeiten der IT-Unterstützung

für Forschungskooperationen vor. Prof. Tadeusz Czachorski von der Universität Gliwice diskutierte neue Ansätze zur Leistungsbewertung von Rechnernetzen und Kommunikationsprotokollen.

Auszeichnungen

KuVS-Preis 2015 für Sebastian Böhm

Sebastian Böhm ist für seine Masterarbeit „IEEE 802.15.4 Sensornetz-Emulation am Praxisbeispiel RoSeNet“, die in Kooperation mit der Firma Dresden Elektronik durchgeführt wurde, mit dem KuVS-Preis 2015 ausgezeichnet worden. Die Fachgruppe "Kommunikation und Verteilte Systeme" (KuVS) der Gesellschaft für Informatik (GI) zeichnet jedes Jahr die beste Dissertation, die beste Masterarbeit und die beste Bachelorarbeit unter allen im letzten Jahr abgeschlossenen Arbeiten im Fachgebiet aus. Sie vereint die Lehrstühle für Rechnernetze und Verteilte Systeme von Universitäten und Hochschulen in Deutschland und der Schweiz und agiert dabei als Interessenvertretung und Kommunikationsplattform für Wissenschaftler und Forscher.

3. Platz beim Best Paper Award IEEE Symposium Series on Computational Intelligence

Das Paper

Franka Schuster, Andreas Paul, René Rietz, Hartmut Koenig
"Potentials of Using One-class SVM for Detecting Protcol-specific Anomalies in Industrial Networks"

hat beim Best Paper Award des IEEE Symposium Series on Computational Intelligence (http://ieee-ssci.org.za:8080/), das vom 8. bis 10. Dezember in Kapstadt/Südafrika stattfand, den 3. Platz belegt. Der Preis wurde über alle 256 akzeptierten Paper, verteilt auf 8 Konferenzen, vergeben. Das Paper ist ein Ergebnis unseres BMBF-Projekts INDI (Intelligente Intrusion Detection Systeme für Industrielle Netze).