



## **TOP 9.1   BERICHTE UND BESCHLUSSVORLAGEN DER FACHBEREICHE**

### **Jahresbericht 2005: Fachbereich Sicherheit – Schutz und Zuverlässigkeit**

#### **Arbeiten des Fachbereichs Sicherheit im Jahr 2005**

Der Fachbereich Sicherheit hatte sich für das Jahr 2005 folgende Arbeitsschwerpunkte gesetzt:

- Durchführung der Sicherheit 2005 in Regensburg
- Vorbereitung der FB-Tagung „Sicherheit 2006“ in Magdeburg
- Verstärkte Darstellung des Fachbereichs in Publikationen
- Weitere Aktivitäten werden im Rahmen der Leitungskreistreffen (nächstes Treffen geplant in März.2006 in Bonn) diskutiert und beschlossen.

Die Fachbereichsleitung traf sich 2005 zweimal zu einer gemeinsamen Sitzung. Vielen Dank an die Organisatoren Matthias Jänichen, PERCOMP Verlag Hamburg und Prof. Francesca Saglietti, Univ. Erlangen.

Erste Ergebnisse der Arbeiten des Editorial Boards sind Veröffentlichungen aus Fachbereichsgruppen im Informatik Spektrum.

Die FB-Seiten wurden in den Rahmen der GI-Seiten integriert. Vielen Dank, Hr. Weber.

Auch in 2005 kann die Jahrestagung des Fachbereichs, durchgeführt unter Leitung von Prof. Federrath in Regensburg, wieder als Erfolg verbucht werden. Das Themenspektrum der Tagung umfasste u.a. Kryptographie und Steganographie, Praktische Sicherheit, Zugriffskontrolle, Fragen der Modellierung, Spezifikation und Verifikation von Schutzmechanismen, Datenschutz und Anonymität im Internet, Intrusion Detection sowie IT-Forensik. Es wurden in mehr als 60 Vorträgen neueste wissenschaftliche Erkenntnisse über Sicherheitstechnologien vorgestellt und in zwei Diskussionsrunden über Fragen der Strafverfolgung im Internet und Monokulturen im Soft- und Hardwarebereich mit den damit verbundenen Sicherheitsrisiken debattiert. Die wissenschaftliche Tagung wurde ergänzt durch die IT-Security-Kompetenz regionaler Unternehmen. In einem Regionalforum mit Vorträgen und Industrieausstellung informierten Experten aus der IT-Wirtschaft über aktuelle Entwicklungen in der Branche. Zehn Unternehmen aus dem Bereich der IT-Sicherheit präsentieren ihre Produkte.

Die nächste Jahrestagung findet vom 20.-22. Februar an der Otto-von-Guericke Universität in Magdeburg (Organisationsleitung: Prof. Jana Dittmann; [www.sicherheit2006.de](http://www.sicherheit2006.de)) statt. Das Programm umfasst

- interessante Vorträge auf der Haupttagung;
- Special Session zu Safety sowie Sicherheit in VoIP;
- Workshops zu Kryptographie und Qualifizierten elektronischen Signaturen in Theorie und Praxis;
- Tutorials zu IT-Grundschutz und Zugriffsmanagement;
- Mini-Workshops zu "Sicherheit und Automotive" und "Audio Watermarking Benchmarking".

### **Organisation des Fachbereichs Sicherheit**

Sprecher: Manfred Reitenspiess, Fujitsu Siemens Computers, München;  
Stellvertretung: Isabel Münch, Bundesamt für Sicherheit in der Informationstechnik, Bonn;

Kai Rannenber, Univ. Frankfurt wurde als Fachexperte berufen als ständiger Vertreter des Fachbereichs im PAK Datenschutz und Sicherheit.

Die Organisation des Fachbereichs blieb gegenüber 2004 nahezu unverändert. Die Fachgruppe KRITIS wurde von Dr. Stein, BSI mit außerordentlichem Engagement ins Leben gerufen und im März 2005 vom Fachbereich bestätigt. Leider mussten wir im Herbst von Dr. Stein, viel zu früh, Abschied nehmen.



Die Fachgruppen und ihre SprecherInnen zum Ende 2005:

ENCRESS	European Network of Clubs for Reliability and Safety of Software-Intensive Systems <a href="http://www11.informatik.uni-erlangen.de/Kooperationen/Encress/index.html">http://www11.informatik.uni-erlangen.de/Kooperationen/Encress/index.html</a>	<b>Francesca Saglietti</b>	Karl-Erwin Großpietsch
FERS	Fehlertolerierende Rechensysteme	<b>Karl-Erwin Großpietsch</b>	Udo Voges
Ada	Ada	<b>Peter Dencker</b>	Hubert Keller
SECMGT	Management von Informationssicherheit	<b>Helmut G. Stiegler</b>	Wolfgang Behnsen
SIDAR	Erkennung und Beherrschung von Vorfaellen der Informationssicherheit	<b>Ulrich Flegel</b>	Detlef Günther
FoMSESS	Formale Methoden und Software Engineering für Sichere Systeme	<b>Jan Jürjens</b>	Thomas Santen
NETSEC	Sicherheit in Mobil- und Festnetzen	<b>Matthias Jänichen</b>	Dogan Kesdogan
BIOSIG	Biometrik und Signaturen	<b>Petra Wohlmacher</b>	Christoph Busch
KRYPTO	Angewandte Kryptologie	<b>Erik Zenner</b>	Ulrich Kühn
STEWA	Steganographie und digitale Wasserzeichen	<b>Eckhard Koch</b>	Jana Dittmann
ECOM	E-Commerce, E-Government und Sicherheit	<b>Rüdiger Grimm</b>	Kai Rannenberg

Gliederung	Kürzel	Okt 05	Dez 04
FG10.00.01	Ada-SICHER	6	7
FG10.00.02	KRYPTO	170	133
FG10.00.03	BIOSIG	165	139
FG10.00.04	PET	134	107
FG10.00.05	ECOM	235	195
FG10.00.06	ENCRESS/SI	54	48
FG10.00.07	SIDAR	172	140
FG10.00.08	EZQN	122	101
FG10.00.09	FERS/SICHE	19	20
FG10.00.10	FoMSESS	146	124
FG10.00.11	SECMGT	213	173
FG10.00.13	NETSEC	248	217
FG10.00.14	STEWA	96	78
FG10.00.16	KRITIS	42	0

PET	Datenschutzfördernde Technik (Privacy Enhancing Technologies)	<b>Marit Hansen</b>	Peter Weiss
EZQN	Evaluation, Zertifizierung, Qualitätssicherung, Normung	<b>Kai Rannenberg</b>	Peer Reymann
KRITIS	Kritische Infrastrukturen	<b>Dirk Schadt</b>	Bernhard M. Hämmerli

## Mitgliederzahlen der Fachgruppen

Hinweis: Bei Fachgruppen mit Mehrfachzuordnung zu einem FB (Ada, FERS, ENCRESS) zeigt die Zählung nur die Primäranmeldung beim FB-Sicherheit. Daraus erklären sich auch die niedrigen gezeigten Mitgliederzahlen.  
Hinweis: Kritis Mitgliederstand vom 12. Januar 2006-01-12



## Ziele für das Jahr 2006

Die Ziele für 2006 sollen am nächsten Treffen der FB-Leitung (26. März 2006 in Bonn) diskutiert und beschlossen werden. Erste Themenvorschläge sind:

- Mitarbeit im Jahr der Informatik
- Mittelfristige Ausrichtung des Fachbereichs nach Abschluss der Aufbauphase

## Die Arbeiten der Fachgruppen im Einzelnen

### Ada-Sicher

13.–14. Okt. 2005	Der <b>Workshop "Zuverlässigkeit in eingebetteten Systemen"</b> mit insgesamt 10 Vorträge wurde an der RWTH Aachen abgehalten. Es gab 30 Teilnehmer. In zwei eingeladenen Vorträgen von Tucker Taft und Erhard Plödereder wurde der neue Sprachstandard Ada 2005 vorgestellt. Der Tagungsband ist in der Reihe Softwaretechnik des Shaker Verlags erschienen (ISBN 3-8322-4522-7).
-------------------	--

Personalien (Wahlen):

Die Wahl zum Leitungsgremium der Fachgruppe Ada fand im Rahmen des Oktoberworkshops am 14. Oktober 2005 statt. Das neue Leitungsgremium setzt sich wie folgt zusammen:

- Sprecher der Fachgruppe: Peter Dencker, Aonix GmbH
- Stellvertretender Sprecher: Hubert Keller, FZ Karlsruhe
- Andreas Thiel, SUZ Manching
- Peter Hermann, Universität Stuttgart
- Michael Tonndorf, CSC PLOENZKE AG

## KRYPTO

Allgemeines

- Es wurde ein kurzes Mustercurriculum für Kryptographie erarbeitet. Dabei handelt es sich vorläufig um einen Minimalkonsens. Eine Erweiterung zu einem vollständigen Curriculum (mehr Details, optionale Elemente) ist angedacht.
- Eine Webseite, die einen Überblick über die deutschen Krypto-Lehrstühle gibt, ist derzeit in Arbeit. Die Seite wird offen gestaltet, so dass Lehrstühle ihre Einträge selbst mitgestalten können.
- Der Workshop „Angewandte Kryptographie“, der im Rahmen der „Sicherheit 2006“ stattfindet, wurde vorbereitet.

31. März 2005	Der 2. Kryptotag wurde an der Universität Ulm abgehalten. Es gab 24 Teilnehmer und 9 Vorträge.
5. – 7. Juli 2005	WEWoRC (West European Workshop on Research in Cryptography) wurde in Kooperation mit Royal Holloway London und KU Leuven erstmalig abgehalten. Der Workshop war international ausgerichtet und richtete sich vor allem an junge Wissenschaftler. Es gab 80 Teilnehmer und 40 Vorträge, von denen etwa ein Dutzend im Tagungsband veröffentlicht wurden.
15. September 2005	Der 3. Kryptotag wurde an der TU Darmstadt abgehalten. Es gab 35 Teilnehmer (davon 20 nicht aus Darmstadt) und 13 Vorträge. Der Kryptotag scheint also etabliert zu haben.

## BIOSIG

6. April 2005	Workshop "Qualifizierte elektronische Signaturen in Theorie und Praxis" (QSIG 2005): Workshop auf der Fachkonferenz Sicherheit 2005 in Regensburg
21. Juli 2005	Jährlicher Workshop im Rahmen des CAST-Forums in enger Kooperation zwischen dem CAST-Verein, der Fachgruppe BIOSIG der Gesellschaft für Informatik und dem Bundesamt für Sicherheit in der Informationstechnik



Personalien (Wahlen, Sprecher/innenwechsel...):

Die Wahl zum Leitungsgremium der Fachgruppe BIOSIG fand im März 2005 statt. Das neue Leitungsgremium setzt sich zusammen wie folgt:

- Sprecherin der Fachgruppe: Petra Wohlmacher, Bundesnetzagentur
- Stellvertretender Sprecher: Christoph Busch, FH Darmstadt
- Presse- und Technikwart: Victor-Philipp Busch, Uni Hamburg
- Wart für Wissenschaft, Forschung und Lehre: Arslan Brömme, Uni Magdeburg
- Kassenwart: Till Teichmann, Hypovereinsbank
- Organisation und Koordination von Workshops, Tagungen, Arbeitsgemeinschaften und der BIOSIG:  
Till Teichmann, Hypovereinsbank;  
Detlef Hühnlein, secunet

## **PET**

6. April 2005	Workshop „Privacy Respecting Incident Management - PRIMA 2005“ ( <a href="http://www.gi-fb-sicherheit.de/fg/sidar/prima2005/">http://www.gi-fb-sicherheit.de/fg/sidar/prima2005/</a> ) in Regensburg im Rahmen der „Sicherheit 2005“, organisiert gemeinsam mit der FG SIDAR; Publikation der Tagungsbeiträge in der DuD 07/2005, Spezialheft zu Privacy Respecting Incident Management, als Gasteditoren: Ulrich Flegel, Marit Hansen und Michael Meier
---------------	--

Personalien:

- Sprecherin der Fachgruppe: Marit Hansen <marit.hansen@aiki.de>
- Stellvertretender Sprecher der Fachgruppe: Stefan Weiß <stefanweiss@deloitte.de>
- Weitere Mitglieder der Fachgruppenleitung: Ulrich Flegel, Dogan Kesdogan, Kai Rannenberg, Peer Reymann, Karin Schuler

## **ECOM**

30.11.-2.12.2005	3. Virtual Goods-Workshop (GI FG ECOM und IFIP WG 6.9) in Florenz im Rahmen der AXMEDIS-Konferenz.
14.-15. April 2005	XML-Signatur-Workshop in Ilmenau
April 2005	1. FG-Treffen bei der Sicherheit 2005 in Regensburg mit Referaten über E-Commerce und E-Wahlen.

Verschiedenes: Begleitung der elektronischen GI-Präsidiums- und Vorstandswahlen im Expertengremium durch die ECOM-Mitglieder Volkamer und Grimm. Insbesondere Wahlüberwachung am 9.12.2005 in Kassel bei Micromata.

## **ENCRESS**

5.-8- April 2005	Jahrestagung Sicherheit 2005, Regensburg
28. - 30. September 2005	24th International Conference on Computer Safety, Reliability and Security (SAFECOMP 2005) in Zusammenarbeit mit EWICS TC7 und dem europäischen Netzwerk ENCRESS Fredrikstad (N)

Verschiedenes: Eine Mitgliederversammlung der Fachgruppe, anlässlich derer das Leitungsgremium gewählt wurde, fand am 24. Oktober 2005 statt.



## SIDAR

02.-03.März 2004	12. DFN CERT-Workshop "Sicherheit in vernetzten Systemen", Hamburg, Typ d (u.a. Beteiligung im Programmkomitee, die Anzahl der SIDAR-Vertreter im Programmkomitee wurde von 2 auf 6 erhöht), <a href="http://www.cert.dfn.de/events/ws/2005/">http://www.cert.dfn.de/events/ws/2005/</a> , Tagungsband ISBN 3-00-015369-1, mehr als 300 Teilnehmer
06.April 2005	Workshop PRIMA "Privacy Respecting Incident Management" im Rahmen der FB-Tagung "Sicherheit 2005", Regensburg, Typ a1, <a href="http://www.gi-fg-sidar.de/prima2005/">http://www.gi-fg-sidar.de/prima2005/</a> , erschienen in einem Themenheft der Zeitschrift DuD - Datenschutz und Datensicherheit, s.u. Veröffentlichungen, mehr als 60 Teilnehmer
07.-08.Juli 2004	2. DIMVA-Konferenz der FG "Detection of Intrusions and Malware, and Vulnerability Assessment", Wien, Typ a1, <a href="http://www.dimva.org/dimva2005/">http://www.dimva.org/dimva2005/</a> , erschienen in LNCS Nr. 3548 s.u. Veröffentlichungen, 51 Beitragseinreichungen aus 18 Ländern, ausgewählt für den Tagungsband: 14 (27%), mehr als 90 Teilnehmer
22. Juli 2005	Workshop SKVU "Sicherheit in komplexen, vernetzten Umgebungen" im Rahmen der GI-Jahrestagung "Informatik 2005", Bonn, Typ a1, <a href="http://www.dimva.org/skvu2005/">http://www.dimva.org/skvu2005/</a> , Beiträge erschienen in LNI als P-68, "Informatik 2005 - Informatik LIVE!" Band 2, Armin B. Cremers et al. (Hrsg.), ISBN 3-88579-397-0, mehr als 30 Teilnehmer

### Personalia:

- Leitungsgremium:
  - Sprecher: Ulrich Flegel (Universität Dortmund)
  - Stv. Sprecher: Detlef Günther (Volkswagen AG, CERT-VW)
  - Roland Büschkes (T-Mobile)
  - Oliver Göbel (Universität Stuttgart, RUS-CERT)
  - Oliver Heinz (arago AG)
  - Marc Heuse (n.runs)
  - Michael Meier (BTU Cottbus)
  - Jens Nedon (ConSecur GmbH)
  - Dirk Schadt (Computer Associates)
- Fachgebietsverantwortung:
  - Forensik J. Nedon, D. Schadt, D. Mauersberger
  - Incident Management D. Günther, O. Göbel
  - Intrusion Detection R. Büschkes, M. Meier
  - Verwundbarkeitsanalyse M. Heuse, O. Heinz, O. Goebel
  - Malware J. Nedon, D. Schadt, T. Dirro
- Presse-Kontakte:
  - Oliver Heinz Vulnerability Assessment
  - Oliver Göbel Vulnerability Assessment, Incident Management
  - Michael Meier Intrusion Detection
  - Ulrich Flegel Intrusion Detection
  - Dirk Schadt Forensik, Malware

### Veröffentlichungen:

- Detection of Intrusions and Malware & Vulnerability Assessment, Klaus Julisch, Christopher Kruegel (Hrsg.), 2. Internationale GI FG  
SIDAR Konferenz DIMVA 2005, 7.-8. Juli 2005 in Wien, Lecture Notes in Computer Science (LNCS), Nr. 3548, Springer (2005), ISBN 3-540-26613-5, 48,15 Euro
- DuD-Themenheft "Incident Management", Ulrich Flegel, Marit Hansen, Michael Meier (Hrsg.), Datenschutz und Datensicherheit, Vol. 29, No. 7, Juli 2005, Vieweg, ISSN 0724-4371

### Weiteres:

- Beteiligung von Fachgruppen-Mitgliedern am Source-Code-Review der Software für die elektronische Vorstands- und Präsidiumswahl der GI in 2005



- Web-Seiten der Fachgruppe neu aufbereitet
- Zugriff auf Fachgebiets-Content vorbereitet
- Logo Fachgruppe SIDAR entworfen
  
- Logo Tagung IMF entworfen
- Logo Workshop PRIMA entworfen
- Bündelung der Publikationskanäle der Fachgruppe vorbereitet, u.a. Kooperation mit IO-Port auch im Hinblick auf gesamten Fachbereich Sicherheit vorbereitet
- Flyer Fachgruppe SIDAR vorbereitet

## **EZQN**

5.-8. April 2005	Beteiligung an der Tagung "Sicherheit 2005" (Regensburg) mit 1) Eingeladener Vortrag: Informationssicherheit und Standardisierung (Roland Müller, Obmann DIN NI-27) 2) EZQN-Mini-Workshop
------------------	---

## **Fehlertolerierende Rechensysteme**

10./11. März 2005	Frühjahrs-Treffen des Diskussionskreises Fehlertoleranz in München mit ca. 25 Teilnehmern.
5.-8. April 2005	Beteiligung an Fachtagung "Sicherheit" des FB Sicherheit in Regensburg;
22.-24. April 2005	Beteiligung an der European Dependable Computing Conference in Budapest
	im Zusammenhang mit der internationalen Konferenz IPDPS 2005 in Denver abgehaltene Workshop on Dependable Parallel, Distributed and Network-centric Systems DPDNS 2005 (Workshop Chair: Prof. Maehle).

## **FoMSESS**

2005	FG Treffen 2005 in Kiel (Lehrstuhl Thomas Wilke), ca. 35 Teilnehmer, eingeladener Vortrag Datenschutzbeauftragter des Landes Schleswig-Holstein, Dr. Thilo Weichert
	WITS 2005 @ POPL 2005 (Long Beach, California): Mit-Organisation und Mit-Leitung in Zusammenarbeit mit IFIP WG 1.7 und ACM SIGPLAN
	CSDUML 2005 (co-located mit SAFECOMP 2005) (Fredrikstad, Norway): Organisation und Leitung in Zusammenarbeit mit preciseUML Arbeitsgruppe
	Workshop Modellierung 2005 (Heidelberg): Mit-Trägerschaft als Fachgruppe und aktive Teilnahme von FG-Mitgliedern
	Konferenz Sicherheit 2005 / 2006: Beiträge von FG-Mitgliedern, Angebot der Organisation einer Session / Tutorial

## **SECMGT**

28. Januar 2005	Frankfurt-Niederrad : Operatives Risiko-Management und IT Sicherheits-Management
13. Juni 2005	München bei BMW: Outsourcing und IT-Sicherheits-Management
12. Oktober 2005	Frankfurt-Niederad: Awareness, Motivation, Schulung

## **NETSEC**

Die Arbeit der Fachgruppe war in 2005 im wesentlichen durch VoIP geprägt. Ein Treffen im Juni 2005 zeigte erhebliche Mängel bei Design und Implementierung von VoIP-Systemen. Es wurde eine Arbeitsgruppe (AG VoIP) ins Leben gerufen. Die Zusammenfassung des Treffens wurde auf der Systems 2005 im Rahmen des "5 vor 12"-

## PRÄSIDIUMSSITZUNG AM 26. UND 27. JANUAR 2006 IN BENSBERG



Forums präsentiert und fand allgemeine Zustimmung bei anderen Experten. Die Fachgruppe hat zur Sicherheit 2006 eine "Special Session VoIP" eingereicht.

Personalien:

Sprecher Matthias Jänichen  
stv. Spr. Dogan Kesdogan  
LG Ammar Alkassar, Hannes Federrath, Klaus Plöbl, Kai Rannenberg

## STEWA

Stewa-Treffen auf der Sicherheit 2005, April in Regensburg

Beitrag für das Informatik Spektrum: Dittmann/Franz/Schneidewind: Steganographie und Wasserzeichen:  
Aktueller Stand und neue Herausforderungen

## KRITIS

19. Sept. 2005	Symposium "CIP Europe 2005" während der "Informatik2005" (Begleitung der GI Pressekonferenz da KRITIS als eines der Kernthemen gewählt wurde)
3.-4. Nov. 2005	"IWCIP2005" International Workshop on Critical Infrastructure Protection in Kooperation mit IEEE

18.2. Vorstellung und Gründung der FG KRITIS bei der FBSEC Sitzung in Hamburg

Personalien:

Sprecher Dirk Schadt (CA)  
Leitung Prof. Dr. Stephen Wolthusen (Gjovik University College)  
Prof. Dr. Bernhard Hämmerli (HTA Luzern)  
Paul Friessem (Fraunhofer SIT)  
Dr. Willi Stein (BSI) verstarb am 28. Oktober 2005

2006-01-12 rei