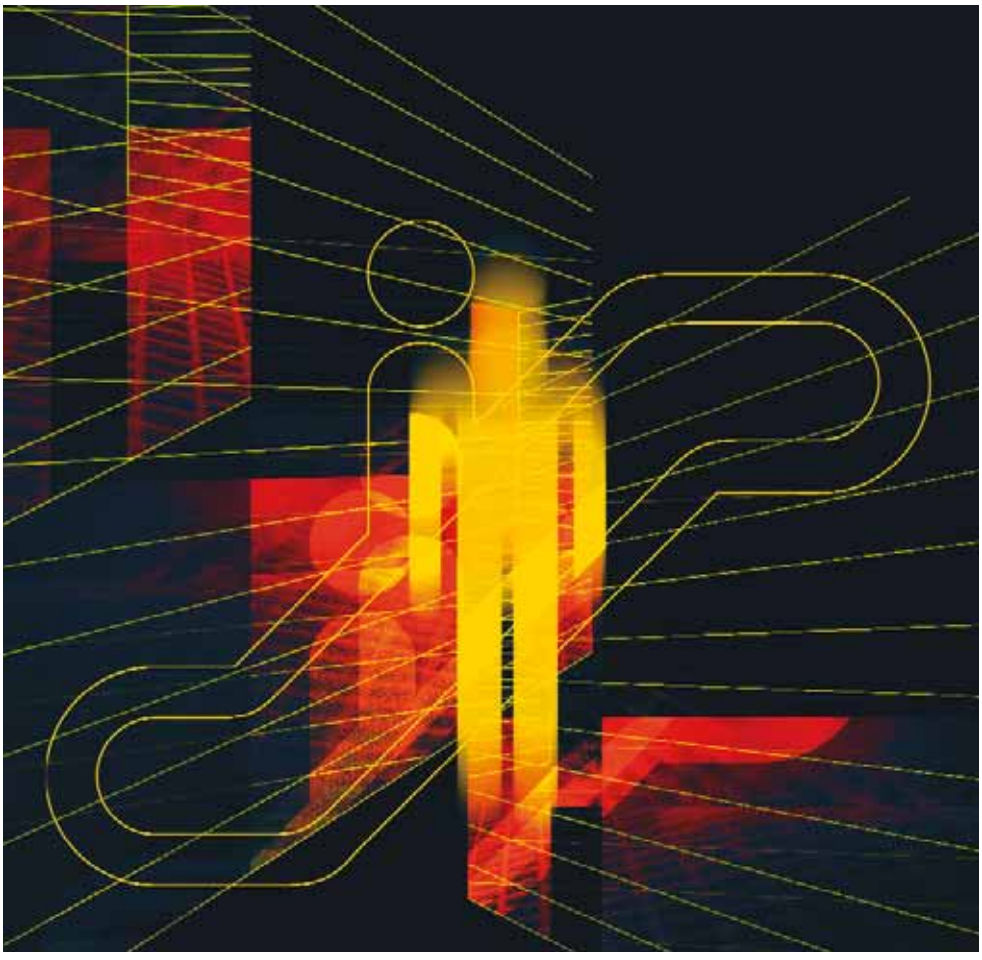
Gemeinsame Arbeitskonferenz: GI | OCG | BITKOM | SI | TeleTrusT

D·A·CH Security

Heinrich-Heine-Universität Düsseldorf | 28. und 29. März 2006



HEINRICH HEINE
UNIVERSITÄT
DÜSSELDORF

Aktuelle Informationen: http://syssec.uni-klu.ac.at/DACHSecurity2006/

syssec secure IT UNIVERSITÄT KLAGENFURT Microsoft secunet

Dienstag • 28. März 2006

08.30 Uhr **Registrierung, Kaffee und Tee**

09.20 Uhr **Begrüßung und Überblick** | **S. Olbrich · T. Faber · P. Horster**

Elektronische Rechnungen • Leitung: R. Posch — A

09.35 Uhr **Signaturformate für elektronische Rechnungen** — **D. Hühnlein**, secunet Security Networks AG; **U. Korte**, BSI
- Elektronische Rechnungen
- Signaturalgorithmen und Signaturformate
- Signaturformate in der Praxis
- Welches Signaturformat ist wofür geeignet?
- Ausgewählte praxisrelevante Beispiele

10.00 Uhr **Labeled Transition System für eInvoicing** — **G. Lindsberger**, XiCrypt GmbH; **G. Fließ**, Campus02
- Rahmenbedingungen von eBilling
- Aspekte von eInvoicing
- Grundlagen der technischen Umsetzung
- Software-Architektur der Implementierung
- Anwendung beim Kunden

10.25 Uhr **Sichere PDF-Rechnungen** — **G. Jacobson**, Secardeo GmbH
- Sicherheitsaspekte elektronischer Rechnungen
- Digitale Signatur mit Acrobat und PDF
- PDF-Signatur- und Verifikationsserver
- Autorisierung von PDF-Rechnungen
- Automatisierte Prüfung von Rechnungsinhalten

10.50 Uhr **Pause – Zeit für Gedankenaustausch**

Dokumentenmanagement • Leitung: N. Pohlmann — A

11.20 Uhr **Realisierung eines sicheren zentralen Datenrepositories** — **C. Stingl**, **D. Slamanig**, **D. Rauner-Reithmayer**, **H. Fischer**, Fachhochschule Technikum Kärnten
- Gesundheitsdatenrepository – Chancen und Risiken
- PKI im Gesundheitswesen
- Formate zur sicheren Datenspeicherung
- Rollenunabhängiges Berechtigungssystem
- Erfahrungen, Ergebnisse und Ausblick

11.45 Uhr **Wie Sie alle Exemplare vertraulicher Dokumente wiederfinden** — **R. Krüger**, **S. Billen**, MediaSec Technologies GmbH; **U. Pinsdorf**, Fraunhofer IGD
- Distributionsflusskontrolle
- Privatsphäre
- Vertraulichkeitsklassifizierung
- Digitale Wasserzeichen
- Mobile Agentenplattform

12.10 Uhr **Key Management für partielle Verschlüsselung von XML-Dokumenten** — **F. Kollmann**, Universität Klagenfurt
- Partielle Verschlüsselung von XML-Dokumenten
- Key Management zur Realisierung von Zugriffsstrukturen
- Vererbung von Zugriffsrechten innerhalb von Teilbäumen
- Generelles Konzept zur Ableitung von Schlüsseln
- Basismechanismen zur Realisierung des Konzeptes

12.35 Uhr **Gemeinsame Mittagspause**

Elektronische Geschäftsprozesse • Leitung: H. Reimer — A

13.35 Uhr **Sectet: Ein Framework für sichere Prozesse** — **M. Hafner**, **R. Breu**, Universität Innsbruck; **A. Nowak**, ARC Seibersdorf
- Model Driven Security
- Sicherere unternehmensübergreifende Prozesse
- eGovernment
- Web Services – Standards und Technologien
- Service Oriented Architectures

Dienstag • 28. März 2006

14.00 Uhr **Geschäftsprozessorientiertes Identity Management erlaubt Compliance** — **A. Kern**, **M. Kuhlmann**, **C. Walhorn**, Beta Systems Software AG

- IT Risk Management und Identity Management
- Verwaltung von Benutzern und Zugriffsrechten
- Definition klarer und nachvollziehbarer Administrationsprozesse
- Durchsetzung und Kontrolle benutzerbezogener Sicherheitsrichtlinien
- Voraussetzungen eines effektiven Identity Audit

14.25 Uhr **eBilling-Szenarien in Theorie und Praxis** — **D. Hühnlein**, secunet Security Networks AG, **U. Korte**, BSI

- Rechtliche Rahmenbedingungen
- Zulässige Abrechnungsszenarien
- Praxisorientierte Rahmenbedingungen
- Buchungsbestätigung bei der dba Luftfahrtgesellschaft mbH
- Provisionskonto-Abrechnung bei der Bausparkasse Schwäbisch Hall AG

Konzepte und Modelle • Leitung: P. Frießem — B

13.35 Uhr **Modellierung von IT-Sicherheit: Analyse und Synthese** — **D. Kalmring**, **G. Dzhendova**, Fraunhofer SIT

- Notwendigkeit einer Sicherheitssicht
- Modellierungsmodelle und Methoden
- Sicherheitsanforderungen auf Fachkonzeptebene
- Bewertung, Auswahl und Erweiterung
- Empfehlungen und Beispiele

14.00 Uhr **Fehlermodelle der Fehlertoleranz für die Einbruchstoleranz** — **T. Warns**, **W. Hasselbring**, Universität Oldenburg

- Einbruchstoleranz – Kombination von Fehlertoleranz (FT) und Sicherheit
- Erweiterung der FT-Beeinträchtigungskette
- FT-Fehlermodi für sichere Systeme
- Modelle für stochastisch abhängige Einbrüche
- Herausforderungen für die Einbruchstoleranz

14.25 Uhr **Anbindung von Zertifikatsverzeichnissen** — **G. Jacobson**, Secardeo GmbH

- Interworking von Public-Key-Infrastrukturen
- Anforderungen an Zertifikatsverzeichnisse
- Sicherer Zugriff auf Verzeichnisdienste mit Certificate Proxy
- PKI Konnektivität mit Certificate Broker
- DNS-basierter Repository Locator Service

14.50 Uhr **Pause – Zeit für Gedankenaustausch**

Sicherheitsmanagement • Leitung: G. Bitz — A

15.20 Uhr **IT-Sicherheitsmanagement auf Basis eines Unternehmensmodells** — **F. Innerhofer-Oberperfler**, **R. Breu**, Universität Innsbruck

- Sicherheitsmanagement im Unternehmen
- Nachverfolgbarkeit von Sicherheitsanforderungen
- Modellbasierte Risikoanalyse
- Organisatorische Einbettung des Sicherheitsprozesses
- Überwachung und Steuerung des Sicherheitsmanagements

15.45 Uhr **Krisenanfälligkeit – Indikatoren für BCM und IT Incident Handling** — **R. v. Rössing**, KPMG

- Krisenanfällige und krisenfeste Unternehmen
- Neue Risiken und Krisenfestigkeit
- Auswirkungen auf BCM und Incident Handling
- Erfolgsfaktoren und Warnindikatoren
- Ausblick

16.10 Uhr **Standardisierte Policy Assurance – eine Vereinfachung?** — **S. Wappler**, noventum consulting GmbH, **W. Fang**, The Boeing Company

- Bilaterale Vereinbarungen
- Multilaterale Vereinbarungen
- Audit und Auditor
- Veröffentlichung der Reports und Zertifizierungen
- Vorteile der Lösung

16.35 Uhr **EIM – Darstellung des unternehmensweiten Sicherheitsstatus** — **G. Wagner**, SAP AG

- EIM (Enterprise Integrity Management) – Ziele und Methodik
- Ermittlung und Darstellung des Sicherheitsstatus eines Unternehmens
- Berechnung der Höhe von sicherheitsrelevanten Risiken
- Monitoring von Sicherheitsaspekten der Regulatory Compliance
- Simulation der Auswirkungen von Projekten und Return on Investment

WLAN Mobilität und Endgeräte • Leitung: P. Schartner — B

15.20 Uhr **Einsatz mobiler Endgeräte – Risiko oder Chance** — **M. Bock**, Teleca Systems GmbH; **A. Philipp**, Utimaco Safeware AG; **S. Wappler**, noventum GmbH

- Klassifizierung von mobilen Endgeräten
- Potentielle Bedrohungen
- Generelle und spezielle Risiken und Gegenmaßnahmen
- Einteilung Eigentumsverhältnis vs. Einsatzzweck
- Checkliste der Sicherheitsmaßnahmen

15.45 Uhr **WLAN-Sicherheit von WEP bis CCMP** — **E. Eren**, Fachhochschule Dortmund; **K.-O. Detken**, DECOIT GmbH

- Hintergrund und Problemstellung
- Sicherheitsmechanismen und Verfahren für WLANs
- Sicherheitslücken, Angriffe und Angriffstools
- Vergleich der Verfahren
- Gesamtbewertung

16.10 Uhr **Untersuchung des Einsatzes von WLAN-Sicherheitsmaßnahmen** — **D. Fischer**, **D. Stelzer**, TU Ilmenau; **P. Steiert**, NetSys.IT • TeleTrusT

- Maßnahmen zum Betrieb sicherer WLANs
- Einsatzhäufigkeit von Sicherheitsmaßnahmen
- Gründe für den Einsatz bzw. Nichteinsatz
- Unternehmensspezifische Verwendung von Sicherheitsmaßnahmen
- Sensibilisierung von Betreibern und Anwendern

16.35 Uhr **Automatisierte Auswahl von WLAN-Sicherheitsmaßnahmen** — **R. Döring**, NetSys.IT; **D. Fischer**, **D. Stelzer**, TU Ilmenau

- Bedrohungsanalyse der Kopplung von WLAN und Firmennetzwerk
- Maßnahmenkatalog zur Absicherung von WLAN-Infrastrukturen
- Regelwerk zur Verknüpfung von Bedrohungs- und Maßnahmenkatalog
- Webbasierte Applikation zur Bestandsaufnahme beim Nutzer
- Automatisierte Auswahl von Verbesserungsvorschlägen

17.00 Uhr **Ende erster Konferenztag**

19.30 Uhr **Gemeinsames Abendessen**

Partner der Konferenz:

Microsoft GmbH. IT Sicherheit ist für Microsoft ein zentrales Ziel. Trustworthy Computing, eine langfristig angelegte Zusammenarbeit aller relevanten Unternehmensbereiche, soll dazu dienen, dem Anwender Zuverlässigkeit, Schutz seiner Privatsphäre und mehr Sicherheit beim Umgang mit IT-Systemen zu geben. Microsoft Deutschland ist Gründer der Initiative „Deutschland sicher im Netz“, die sich vor allem an Endnutzer richtet. Ziel ist für potenzielle Gefahren im Internet zu sensibilisieren und umfassend darüber zu informieren, wie sich der eigene Online-Schutz schnell und wirksam verbessern lässt. *www.microsoft.com/germany/sicherheit*

secunet Security Networks AG. secunet ist einer der führenden europäischen Anbieter von Produkten und Beratungsleistungen auf dem Gebiet hochkomplexer IT-Sicherheitssysteme. Das Unternehmen stellt mit über 200 Mitarbeitern die komplette Leistungsbandbreite der IT Security zur Verfügung. Kunden erhalten Beratung, Entwicklung und Integration sowie Schulung und Service aus einer Hand. *www.secunet.com*

secure-it.nrw. Die Landesinitiative für mehr Sicherheit und Vertrauen in elektronische Geschäftsprozesse hat das Ziel, innovative Geschäftsprozesse auszubauen und zu fördern. Die Aktivitäten umfassen die Förderung der IT-Sicherheit und der Akzeptanz elektronischer Geschäftsprozesse unter Erschließung innovativer Wachstumsfelder. *www.secure-it.nrw.de*

syssec. Neben Kernkompetenzen in den Bereichen Sicherheitsinfrastrukturen und Angewandte Kryptologie verfügt die Forschungsgruppe Systemsicherheit über Erfahrungen beim Aufbau komplexer sicherheitsrelevanter Systeme in unterschiedlichen Anwendungsfeldern wie Passsystemen, Sportereignissen und Automobilen. *syssec@uni-klu.ac.at*

Fachbereich Informatik. Lehre und Forschung sind theoretisch fundiert und anwendungsorientiert. Ein obligatorisches Praxissemester fördert diese Ausrichtung. Zudem werden das Lehramtsstudium Informatik, das Studium Informationsmanagement und der im Ausbau befindliche Technische Fachbereich unterstützt. In der Forschung kann auf erfolgreiche Projekte mit Partnern aus Wirtschaft und Wissenschaft verwiesen werden. *www.ifi.uni-klu.ac.at*

Mittwoch • 29. März 2006

Sicherheit digitaler Medien • Leitung: I. Münch — A

09.00 Uhr **The MPEG-21 Multimedia Framework: Conversions and Permissions**
- Permissible Adaptation of Digital Media Content
- Rights Expression Language
- Digital Item Adaptation
- Universal Multimedia Access
- Interoperability: MPEG-21

C. Timmerer
H. Hellwagner
Universität Klagenfurt
T. DeMartini
ContentGuard Inc., USA

09.25 Uhr **Praxisnaher koalitionssicherer Fingerabdruckalgorithmus für Bilder**
- Anforderungen an Fingerabdruckalgorithmen
- Beispiele für Koalitionsattacken auf digitale Wasserzeichen
- Ansätze für koalitionssichere Fingerabdruckalgorithmen
- Darstellung eines praxisnahen Fingerabdruckalgorithmus
- Beispielanwendungen

L. Croce-Ferri
M. Steinebach
M. Knoth
Fraunhofer IPSI

09.50 Uhr **Wasserzeichentreue Bildbearbeitung**
- Ansätze zum Integritätsschutz digitaler Bilder
- Zusammenspiel von Schutzmechanismen und Anwendungsumgebungen
- Integration eines inhaltsfragilen Wasserzeichens in einen Bildeditor
- Anforderungen an die Bedienbarkeit
- Bildbearbeitung mit Feedback bei Inhaltsänderungen

M. Steinebach
P. Wolf
V. Hübler
Fraunhofer IPSI

10.15 Uhr **DRM für Multimedia Broadcasts, wie sieht das Pay-TV der Zukunft aus?**
- Globales Pay-TV durch etablierte Standards
- Digitales Rechtemanagement als Herausforderung
- Lizenzmodelle unterschiedlicher Regionen
- Empfangsgeräte – Durchsetzung regionaler Lizenzmodelle
- Lösung ohne Einsatz von Trusted Computing

U. Greveler
Ruhr-Universität Bochum

10.40 Uhr **Pause – Zeit für Gedankenaustausch**

Secure Computing • Leitung: W. Effing — B

09.00 Uhr **Praktische Angriffe auf eingebettete Systeme**
- Gefährdung von Consumer-Elektronik
- Mangelhafte Sicherheitsprüfungen infolge Kostendrucks
- Gefährdungspotenzial aus Hersteller- und Nutzersicht
- Schutzprobleme des Endnutzers
- Das unterschätzte Restrisiko

M. Holzt
Ruhr-Universität Bochum

09.25 Uhr **Seitenkanal-Analysen: Stand der Forschung in der Methodik**
- Analyse der Implementierung von kryptographischen Algorithmen
- Seitenkanäle als Informationsquellen
- Angreifermodelle
- Klassifikation der Methoden
- Prüfkriterien für die Praxis

K. Lemke
C. Paar
Ruhr-Universität Bochum

09.50 Uhr **Zur Sicherheit von neuen Chipkartenbetriebssystemen**
- Merkmale neuer Chipkartenbetriebssysteme wie Java Card 3.0
- Neue Protokolle für die Kommunikation mit Chipkarten
- Mehrläufige Programmausführung (Multitasking, Multithreading)
- Sicherheitsbetrachtung der vorgestellten Merkmale
- Sicherheitsaspekte bei Chipkarten heute und morgen

W. Hinz
S. Spitz
Giesecke & Devrient GmbH

10.15 Uhr **Die vertrauenswürdige Sicherheitsplattform Turaya**
- Hardwaregebundene Sicherheit durch Trusted Computing
- Architektur der Sicherheitsplattform
- Konzepte der Plattform
- Ziele und Problemlösungen
- EMSCB-basierte Applikationen

M. Linnemann
Institut für Internet-Sicherheit
N. Pohlmann
Fachhochschule Gelsenkirchen

10.40 Uhr **Pause – Zeit für Gedankenaustausch**

Mittwoch • 29. März 2006

eGovernment und Recht • Leitung: K.-D. Wolfenstetter — A

11.10 Uhr **Urheberrechtskonforme Gestaltung von Websites**
S. Janisch
Universität Salzburg

- Allgemeine Grundsätze des Urheberrechts
- Einräumung von Nutzungsrechten
- Verwendung von Fremdmaterial
- Links auf fremde Websites mit Urheberrechtsverstößen?
- Rechtsfolgen von Urheberrechtsverletzungen

11.35 Uhr **PDF Signaturen mit der Bürgerkarte**
T. Neubauer
E. Weippl
TU Wien
A. Hollosi
Bundeskanzleramt (A)
Stabsstelle IKT-Strategie

- PDF Signaturen – Signierte Inhalte
- Anzeige von Signaturwerten
- Signaturprüfung anhand des Ausdrucks
- Erkennen signierter Inhalte
- Erzeugen binäridenter PDF Dokumente

12.00 Uhr **Überblick Online-Wahlen**
M. Volkamer
DFKI
R. Krimmer
WU Wien

- Rechtsgrundlagen in Deutschland, Österreich und der Schweiz
- Sicherheitsanforderungen an Online-Wahlsysteme
- Konkrete technische Umsetzungen
- Pilotprojekte in Deutschland, Österreich und der Schweiz
- Offene Fragen und Probleme

Web-Anwendungen und Bedrohungen • Leitung: R. Ackermann — B

11.10 Uhr **Klassifikation der Eigenschaften von Trojanischen Pferden**
S. Kiltz
A. Lang
J. Dittmann
Otto-von-Guericke
Universität Magdeburg

- Trojanische Pferde als reale Bedrohung von IT-Systemen
- Klassifikation zur Unterstützung der Bedrohungsanalyse
- Beispielhafte Analyse unter Verwendung relevanter Eigenschaften
- Gefährdung durch Trojanische Pferde im Automobilsektor
- Praxisbeispiele und Perspektiven

11.35 Uhr **Application Roles in WebSphere Portal**
J. Buchwald
D. Buehler
T. Hurek
H. Waterstrat
IBM Deutschland
Entwicklung GmbH

- Zugriffskontrolle für inhaltlich zusammenhängende Ressourcen
- Modellierung von Rollen auf semantischer Ebene
- Dynamische Zuweisung komplexer Berechtigungen
- Vereinfachte und schnellere Administration der Zugriffskontrolle
- Bessere Unterstützung externer Autorisierungsanbieter

12.00 Uhr **Perspektiven vertrauenswürdiger Aussagen im Semantic Web**
L. Suhrbier
Freie Universität Berlin

- Problem: Vertrauenswürdige Aussagen im Semantic Web
- Autorenbezogene Konzepte
- Modellierung einer semantischen Sicherheitsarchitektur
- PKI-Integration in semantische Inferenzmechanismen
- Anwendungsszenarien

12.25 Uhr **Pause – Gemeinsame Mittagspause**

Biometrie • Leitung: J. Dittmann — A

13.25 Uhr **Digitalisierte eigenhändige Unterschrift im Online-Banking**
N. Repp
R. Berbner
TU Darmstadt
J. M. Lenz
Softpro GmbH & Co. KG

- Authentifizierung von Nutzern und Autorisierung von Transaktionen
- Alternative zu PIN/TAN
- Digitalisierte eigenhändige Unterschrift als biometrisches Verfahren
- Proof-of-Concept durch prototypische Umsetzung
- Multi-Channel Integration mit Hilfe digitaler Unterschriften

13.50 Uhr **Untersuchung der Möglichkeit eines biometrischen On-Pen Matching**
T. Scheidat
C. Vielhauer
Otto-von-Guericke
Universität Magdeburg

- Handschriftdynamik als biometrisches Merkmal
- Authentifikation durch Besitz und Sein
- Herausforderung Smart Pen Technologie
- Konzeption für On-Pen Matching
- Experimentelle Evaluierung

Mittwoch • 29. März 2006

14.15 Uhr **Multimodalität – die bessere Biometrie?**
- Varianten multimodaler Systeme
- Potenzial zur Verbesserung der Erkennungsleistung
- Theoretische Hintergründe
- Konfiguration multimodaler Systeme
- Multimodalität in der Praxis

M. Breitenstein
M. Niesing
secunet Security Networks AG

14.40 Uhr **Pause – Zeit für Gedankenaustausch**

Sichere eMails und Voice over IP • Leitung: T. Obert — A

15.10 Uhr **Austausch verschlüsselter eMails über externe Mailinglisten**
- Sichere Kommunikation via Mail-Gateway – Architektur
- Vorstellung einer Testspezifkation
- Senden und Empfangen verschlüsselter und signierter eMails
- Einbindung der optionalen Dienste LDAP und OCSP
- Vorstellung der Ergebnisse

P. Steiert
NetSys.IT
S. Wappler
noventum GmbH

15.35 Uhr **Sichere elektronische Geschäftsprozesse via Voice over IP**
- Elektronische Geschäftsprozesse via Voice over IP
- Kommunikationssysteme mit integriertem VoIP
- Risikoanalyse der VoIP-Geschäftstelefonie
- Anwender- und Technologie-Sicherheit
- Sicherheitskonzept für VoIP

P. Merten
D. Wenger
S. Teufel
iimt, Universität Freiburg

16.00 Uhr **VoIP-Sicherheit – Status Quo und neue Aspekte**
- Schutzziele und deren Bedeutung in Voice over IP
- Telefoniesysteme – Asterisk und Skype
- Neue Herausforderungen – SPIT
- Mechanismen für Sicherheit in Voice over IP
- Anwendbarkeit und Wirksamkeit von sicherheitsrelevanten Mechanismen

J. Schmitt
R. Ackermann
M. Goertz
R. Steinmetz
TU Darmstadt (KOM)

16.25 Uhr **Konferenzende**

... als Referenten haben sich zusätzlich zur Verfügung gestellt:

- **Sicherheitsaspekte eines mobilen Multimedia-User-Guides**
  S. Gebbensleben · J. Dittmann · C. Vielhauer Otto-von-Guericke Universität Magdeburg
- **Zutrittskontrolle bei internationalen Großveranstaltungen**
  R. Krüger · C. Reuthe MediaSec Technologies GmbH
- **IT-Grundschutz-Assessments nach BSI-Standard 100**
  A. Altrhein TÜV Informationstechnik GmbH
- **Praktische Umsetzung und Evaluation von Wet Paper Codes**
  T. Vogel · M. Touchev · J. Dittmann Otto-von-Guericke Universität Magdeburg
- **Zukunft von Enterprise Rights Management**
  G. Bitz SAP AG

Die Beiträge dieser Referenten finden Sie ebenfalls im Tagungsband zur Konferenz.

Anmeldung & Teilnahmebedingungen

D•A•CH Security 2006

28. und 29. März 2006
Heinrich-Heine-Universität Düsseldorf

via Fax an: ++49 (0)5921-722-493 oder
Online-Formular unter: http://syssec.uni-klu.ac.at/DACHSecurity2006/html/anmeldung.html oder an:

Organisationskomitee D•A•CH Security 2006
Peter Kraaibeek
Bogenstr. 5a
D-48529 Nordhorn
Telefon: ++49 (0)5921-722-490
E-Mail: Peter@Kraaibeek.com

Anmeldung zur Konferenz

Name

Firma

Funktion

Straße

PLZ/Ort

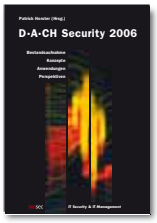
Tel.-Nr.

Fax-Nr.

E-Mail

❑ **Hiermit melde ich mich verbindlich zur Arbeitskonferenz D•A•CH Security 2006 am 28. und 29. März 2006 an der Heinrich-Heine-Universität Düsseldorf an.**

❑ **Ich kann an der Tagung nicht teilnehmen, bestelle aber ein Exemplar des Tagungsbandes zum Preis von € 59.– inkl. MwSt.**



Teilnahmebedingungen

Bei Anmeldung bis zum 24. Februar 2006 beträgt die Frühanmeldegebühr € 285.– zzgl. MwSt. (330,60 €), anschließend beträgt die Teilnahmegebühr € 330.– zzgl. MwSt. (382,80 €).

Die Teilnahmegebühr beinhaltet ein Exemplar des Tagungsbandes (Hardcover mit ISBN), Pausengetränke, Mittagessen an beiden Konferenztagen und ein gemeinsames Abendessen am ersten Konferenztag.

Bei Stornierung der Anmeldung bis 10. März 2006 (Datum des Poststempels) wird eine Bearbeitungsgebühr von € 75.– (inkl. MwSt.) erhoben. Nach dem 10. März 2006 ist die volle Tagungsgebühr zu entrichten. Es ist jederzeit die Benennung einer Ersatzperson ohne zusätzliche Kosten möglich.

Die Teilnahmegebühr überweise ich sofort nach Erhalt der Anmeldebestätigung und Rechnung unter Angabe der Rechnungsnummer auf das Tagungskonto.

Ort und Datum Unterschrift