

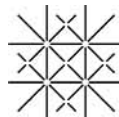
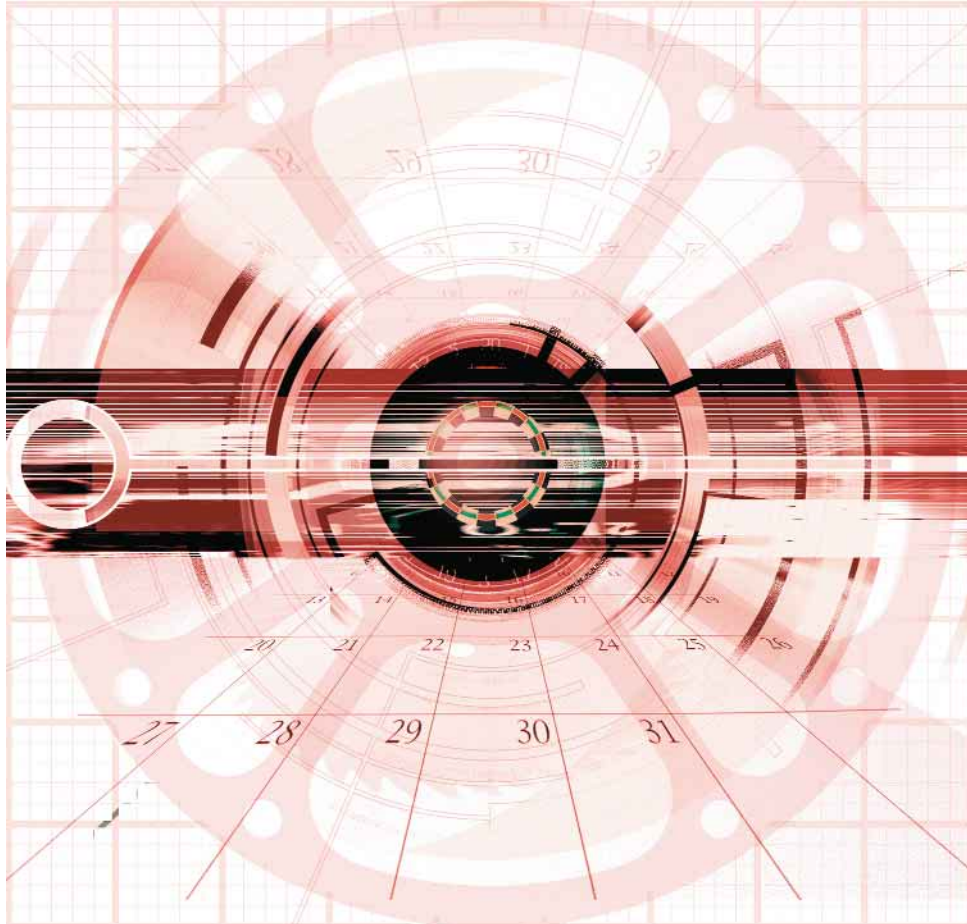


Gemeinsame Arbeitskonferenz: GI | OCG | BITKOM | SI | TeleTrust



D·A·CH Security

Universität Basel | 30. und 31. März 2004



UNI
BASEL

Aktuelle Informationen: <http://syssec.uni-klu.ac.at/DACH2004/>





Dienstag • 30. März 2004

08.30 Uhr Registrierung, Kaffee und Tee

09.20 Uhr Begrüßung und Überblick

Mittelstand und Grundschutz • Leitung: T. Faber

09.35 Uhr IT-Sicherheit im Mittelstand – Anspruch und Wirklichkeit

- Bestandsaufnahme: Wo steht der Mittelstand
- Best Practice: Trend zu pragmatischen Lösungen
- Was kleine und mittlere Unternehmen von IT-Sicherheit erwarten
- Die Hemmschwellen bei den Unternehmen
- Warum es immer noch Verständnisprobleme gibt

M. Pommer

Kesberg, Bütfering
& Partner

10.00 Uhr Elektronische Geschäftsprozesse bei KMU: Stand und Perspektiven

- Charakteristische Kommunikationsbeziehungen
- Schwerpunkte und Lücken
- Integration von IT-Sicherheit in den Gesamtprozess
- Handlungsempfehlungen
- eBusiness Trends – Wie geht es weiter?

P. Frießem

H. Grosse-Onnebrink
Fraunhofer SIT

10.25 Uhr Hilfe zur Selbsthilfe – Das IT-Grundschutzhandbuch

- Prinzipien des IT-Grundschutzhandbuches
- Der Web-Kurs als Einstieg in den IT-Grundschutz
- Leitfaden IT-Sicherheit als Sicherheitsüberblick
- Das IT-Grundschutz-Tool
- Vorteile einer IT-Grundschutz-Zertifizierung

A. Jaschob

BSI

10.50 Uhr Kommunikationspause

Sicherheitsmanagement • Leitung: H. Reimer

11.20 Uhr Ansätze zu einem integrierten Sicherheitsmanagement

- Quick-Wins durch IT-Security mit ITIL
- Toolgestützte Integration der Security Prozesse
- Management operationaler Risiken
- Rollenspezifische Sichten und Themenvernetzung
- Steigerung der Management Attention

T. Kob

HiSolutionsAG

11.45 Uhr Implementierung von Security Policies in offenen Telekollaborationen

- Ein strukturierter Ansatz zur Implementation von Sicherheitspolitiken
- Sicherheitsrelevante Besonderheiten offener Telekollaborationen
- Von Sicherheitsanforderungen zu Policies
- Formale Sicherheitsbeweise
- Ein Rahmen für Enforcement- und Awarenesskomponenten

U. Böttge et al.

Fraunhofer-Institute

D. Rüdiger

ZGDV Rostock

St. Vettermann

TU-Darmstadt

12.10 Uhr Sicherheitsmechanismen unter Berücksichtigung der Risikoentstehung

- Sicherheitsmanagement
- Bedrohungs- und Risikoanalyse
- Modifikation des Anwendungssystems
- Auswahl von Sicherheitsmechanismen
- Tool zur automatisierten Integration von Sicherheitsmechanismen

A. Schönberg

OFFIS

12.35 Uhr Gemeinsame Mittagspause

Outsourcing und Grundschutz • Leitung: S. Teufel

13.35 Uhr Outsourcing unter Sicherheitsgesichtspunkten

- Sicherheitsprobleme beim Outsourcing
- Strategische Planung
- Auswahl eines geeigneten Dienstleisters
- Vertragsgestaltung aus Sicherheitssicht
- Migration und IT-Sicherheit im laufenden Betrieb

M. Mehrhoff

BSI

14.00 Uhr Absicherung von PKI-Outsourcing mittels verteilter digitaler Signaturen

- Risiken beim Outsourcing
- Herkömmlicher Enrollment-Prozess
- Absicherung des Enrollments mit verteilten Signaturen
- Hintergrund: Verteilte RSA-Signatur, verteilte Schlüsselgenerierung
- Praktische Aspekte

T. Straub

TU-Darmstadt

Dienstag • 30. März 2004

14.25 Uhr **Erfahrungen mit der IT-Grundschutz-Zertifizierung**

- IT-Grundschutz als Sicherheitsstrategie
- IT-Grundschutz-Zertifizierung: Vertrauen gegen Nachweis
- Zeitplan und Ressourcenbedarf
- Erfolgsfaktoren und Hindernisse
- Gut heißt noch nicht optimal: Verbesserungspotenzial

A. Alrhein
TÜV Informations-
technik GmbH

Angriffe und Maßnahmen • Leitung: R. Posch

B

13.35 Uhr **Logfilekorrelation – der einzige Weg echte Angriffe zu erkennen**

- Herausforderungen im Umgang mit Logfiles
- Strategien zur Logfilebearbeitung
- Ziele einer Logfilekorrelation
- Stufen der Logfilekorrelation
- Mögliche Szenarien

F. Schneider
SECARTIS AG

14.00 Uhr **SIMS – Simulationsumgebung zur Analyse von Angriffsklassen**

- Simulation zur Aufklärung und Analyse von Angriffen und Maßnahmen
- Angreifer, Opfer und Netzwerke – UML basierte Modelle
- Aufbau der Simulationsumgebung SIMS
- Simulation eines DoS-Szenarios
- Erweiterung auf andere Angriffsklassen und Szenarien

K.M. Bayarou
C. Eckert
Fraunhofer SIT
M. Steiner
TU-Darmstadt

14.25 Uhr **Der Wandel von Intrusion Detection zu Intrusion Prevention**

- Grundlagen
- Verwundbarkeitsmanagement
- Neue Anforderungen
- Innovative Technologien
- Lösungsansätze für die unterschiedlichen Anforderungen

S. Strobel
cirosec GmbH

14.50 Uhr **Kommunikationspause**

Architekturen • Leitung: W. Kühnhauser

A

15.20 Uhr **Schaffung einer Infrastruktur für vertrauenswürdiges eBusiness**

- Sinn einer Bridge Infrastruktur
- Ebenen von Interoperabilität
- Anforderungen an eine Bridge Infrastruktur
- Mindestanforderungen für eine Teilnahme
- Vorstellung von Lösungsmöglichkeiten

S. Wappler
noventum consulting
GmbH
P. Steiert Teletrust
T. Störtkuhl
secaron AG

15.45 Uhr **Adaptive Network Architecture**

- Ein nach Business Anforderungen strukturiertes sicheres Netzwerk
- Flexible, sichere und schnelle Absicherung der IT Infrastruktur
- Migrationswege zu einer gemeinsamen sicheren Infrastruktur
- Zentrales Management der neuen sicheren IT Infrastruktur
- Security Kosteneinsparung durch Adaptive Network Architecture

H. Rank
F. Scheyhing
Hewlett-Packard
GmbH

16.10 Uhr **LDAP-Proxy – einfacher Zugriff auf Verzeichnisdienste**

- Hintergrundinformationen zum Open Source LDAP Proxy
- Vorteile eines LDAP Proxy
- Funktionalität des LDAP Proxy
- Einsatzmöglichkeiten
- Ausblick weitere Entwicklung

Wen Fang
The Boeing
Company
S. Wappler
noventum
consulting GmbH

16.35 Uhr **Architekturanalyse zum sicheren Wireless Zugang in Firmennetze**

- Veränderung der Risikolandschaft durch Wireless LAN
- Sicherheitsrisiken WLAN
- Managebarkeit von sicheren WLAN Installationen
- Aktuelle Topologien im WLAN unter Sicherheitsaspekten
- Sicherheit versus Kosten und Aufwand

L. Gramelpacher
Hoffmann-La Roche
AG Basel
M. Moser
Moser Informatik
Winterthur



15.20 Uhr **Vorfallobarbeitung durch Computer Emergency Response Teams**

- CERT als Teil des Krisenmanagements
- Aufgaben von CERTs im Unternehmen
- Präventive und reaktive Dienstleistungen
- Workflow-Unterstützung für die CERT-Arbeit
- Standards für die Zusammenarbeit von CERTs

M. Weitke
secunet AG

15.45 Uhr **CIRCA Computer Incident Response Coordination Austria**

- WEB of Trust der IP Netzbetreiber
- Nationales Österreichisches Internet Warnsystem (PPP)
- Schutz kritischer Infrastrukturen
- Notfallvorsorge
- Sensortechnik

O. Hellwig
CIRCA Konsortium

16.10 Uhr **Computer Forensik – Mehr als das Kopieren von Festplatten**

- Möglichkeiten der Planung im Vorfeld
- Auswahl der Ermittlungsstrategie
- Der richtige Umgang mit Beweismitteln
- Wo findet man Spuren und was sagen sie aus
- Zusammenführen aller Erkenntnisse

A. Geschonneck
HiSolutions AG

16.35 Uhr **Forensik und Biometrie zur Benutzererkennung**

- Beispiel: Handschrift
- Forensische Schriftanalyse: Grundlagen
- Biometrie: Übertragbarkeit forensischer Verfahren
- Parameterbestimmung: Online-Handschriften
- Evaluierung: Testergebnisse

C. Vielhauer
R. Steinmetz
TU-Darmstadt
T. Scheidat
Uni Magdeburg

17.15 Uhr **Ende erster Konferenztag**

19.30 Uhr **Gemeinsames Abendessen** Dinnerrede: Microsoft EMEA

D. Eckert

Partner der Konferenz:

betasystems **Beta Systems Software** ist ein international tätiger Produkt- und Lösungsanbieter von Qualitätssoftware und Serviceleistungen für das IT-Management. Das Unternehmen verfügt über 20 Jahre Erfahrung in System- und Security-Management für Großunternehmen und IT-Outsourcer. Im Bereich Security Management bietet Beta Systems SAM Jupiter, eine plattformübergreifende Lösung für automatisiertes Identity Management und User Provisioning. www.betasystems.com

manage it **manage it.** Das Premium-Magazin „manage it“ bietet für Entscheider in der Unternehmensführung strategische Analysen und für die Manager der Informationstechnologie fundierte Basisinformationen über die ökonomischen Aspekte der IT. Manage it bietet Information für Top-Manager im Sinne des „mach' es“ und für IT-Spezialisten in Form des „Managen der IT“. www.ap-verlag.de

Microsoft **Microsoft GmbH.** Microsoft hat mit der „Trustworthy Computing Initiative“ das Thema Sicherheit im umfassenden Sinne zur obersten Priorität des Unternehmens gemacht. Mit dieser Initiative beabsichtigt Microsoft Produkte zu entwickeln und anzubieten, die bezüglich Sicherheit, Schutz der Privatsphäre und Zuverlässigkeit zum Referenzpunkt für die gesamte Industrie werden. www.microsoft.com/emea/default.msp

secunet **secunet SwissIT AG.** Die secunet SwissIT ist die Schweizer Tochtergesellschaft der deutschen secunet Security Networks AG, einem führenden europäischen Dienstleister auf dem Gebiet hochkomplexer IT-Sicherheitssysteme. Die Unternehmensgruppe ist herstellerneutral und bietet die komplette Leistungsbandbreite der IT-Security an. Kunden erhalten Beratung, Implementierung, Schulung und Service aus einer Hand. www.swiss-it.ch, www.secunet.com

SECURE IT **secure-it.nrw.2005.** 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

swisscom **Swisscom Enterprise Solutions.** Swisscom Enterprise Solutions bietet umfassende ICT-Lösungen für Geschäftskunden an. Das Kerngeschäft von Swisscom Enterprise Solutions sind Consulting, Implementation und Betrieb von ICT-Infrastrukturen, die auch höchsten Ansprüchen an Zuverlässigkeit und Sicherheit genügen. So werden unter anderem die aus dem Security Operation Center (SOC) angebotenen Dienstleistungen in den Bereichen von Identity und Access Management (Provisioning, PKI und Directories) sowie Perimeter Security (Managed Firewall, IDS, Secure VPN) von international und national tätigen Unternehmen erfolgreich eingesetzt. www.swisscom.com/enterprise-solutions

ZFH **ZFH.** Fernstudium Informatik: Ihre Investition in die Zukunft! Weiterbildungsfernstudium als Diplom-Aufbaustudium mit dem Abschluss Diplom-Informatiker/in (FH) sowie als wissenschaftliche Weiterbildung mit dem Abschluss Hochschulzertifikat. Das Fernstudium kann als Gesamtstudium oder in Form einzelner Module (Dauer jeweils 1 Semester) belegt werden. Als Lehreinheiten stehen u.a. zur Auswahl: IT-Sicherheit, Programmierung, Datenbanksysteme. Nähere Details unter <http://www.zfh.de> und <http://fernstudiumai.fh-trier.de>

Mittwoch • 31. März 2004

Sicherheit in Anwendungen • Leitung: K.-D. Wolfenstetter

A

09.00 Uhr Modellierung von Anwendungssicherheitsdiensten

- Anwendungssicherheitsdienste
- Verknüpfung von Architektur und Sicherheit
- Modelle verteilter Komponenten
- Constraint Models und Metasprachen
- Policy-Modellierung und Role Based Access Control

B. Blobel
P. Pharow
Uni Magdeburg
R. Nordberg
Sahlgrens University
Hospital, Schweden

09.25 Uhr Gesichtserkennung für den geplanten Einsatz in Lichtbildausweisen

- Vergleichende Untersuchung von Gesichtserkennungssystemen
- Gesichtserkennung für den Einsatz mit deutschen Personalausweisen
- Gesichtserkennung auf Basis von Passbildern
- Empfehlungen für zukünftige Reisedokumente
- Feldtest mit über 200 Teilnehmern – Akzeptanzuntersuchungen

A. Albrecht
BSI
M. Breitenstein
secunet AG

09.50 Uhr Zukünftiger Einsatz von Chipkarten im deutschen Gesundheitswesen

- Rechtslage nach dem Gesundheitssystemmodernisierungsgesetz
- Signaturrechtliche Normen bei Gesundheitskarte und Heilberufsausweis
- Datenschutzrechtliche Einschränkungen
- Auskunftsansprüche der Patienten
- Technische Gestaltungsanforderungen

G. Hornung
Uni Kassel

10.15 Uhr Anti-Spam Technologie

- Definition und Hintergründe von SPAM-Mails
- Schäden, die durch SPAM-Mails auftreten
- Verfahren zur Erkennung von SPAM-Mails
- Methoden zur Verhinderung von SPAM-Mails
- Ausblick und Perspektiven

N. Pohlmann
FH Gelsenkirchen

Signaturen und Zertifikate • Leitung: I. Münch

B

09.00 Uhr Spezifikation von X.509-Zertifikatsprofilen unter Benutzbarkeitsaspekten

- Begriff des Zertifikatsprofils
- Probleme und Risiken bei der Spezifikation
- Das etCerte-Konzept
- XML-Beschreibungssprache für Anforderungen an Zertifikatsspezifikationen
- Prototyp und Ausblick

T. Straub
TU-Darmstadt

09.25 Uhr Zielgerichteter Einsatz der digitalen Signatur

- Das Gesamtkonzept entscheidet
- Kriterien zur Auswahl des Signaturverfahrens
- Genehmigung von Medikamentenanforderungen
- Konzeptansatz am Beispiel der deutschen Energiewirtschaft
- Digitale Signaturen als Erfolgsfaktor

B. Weiss
Utimaco AG

09.50 Uhr Vertrauenswürdige digital signierte Zeitstempel

- Notwendigkeit von digitalen Signaturen und Zeitstempeln
- Zeitstempeldienste in einem Trust Center
- Eine Technik zur Erstellung von digital signierten Zeitstempeln
- Anforderungen an einen Zeitstempeldienst
- Verwendung von digital signierten Zeitstempeln in der Praxis

G. Scheer
Utimaco AG

10.15 Uhr Beweiskräftige Langzeitarchivierung elektronisch signierter Dokumente

- Signaturgesetz
- Sicherheitseignung und Neusignierung
- Technische Beweismittel und deren Erhaltung
- Signaturformat und Standardisierung
- ArchiSig-Modell und Ergebnisse

M. Tielemann
DATEV eG

10.40 Uhr Kommunikationspause



Mittwoch • 31. März 2004

Datenschutz • Leitung: S. Janisch

A

11.10 Uhr Common Criteria und Datenschutz – Nicht länger eine flüchtige Affäre

- Problemaufriss
- IT-Sicherheit versus Datenschutz
- Komplexität des Datenschutzes
- Datenschutz-Qualifizierung gemäß Common Criteria
- Sicherheitsanforderungen und Schutzprofilbildung

B. Weghaus
TÜViT GmbH

11.35 Uhr Datenschutz in der Wirtschaft

- Umgang mit Kundendaten und Datenübermittlung
- Datenschutz in Österreich und Deutschland
- Sicherheitsrichtlinien
- Datensicherheitsmechanismen
- Informationsverbund

M.Trappitsch
W. Goller
evolaris
Competence Center

12.00 Uhr Datenschutz bei personalisierten Marketingstrategien

- Customer Relationship Management (CRM) verbreitet sich
- Data Warehouse und Data Mining ermöglichen detaillierte Kundenprofile
- Personalisierungsstrategien für Marketing und Risk Scoring
- Derzeitige Instrumente des Datenschutzes sind unzureichend
- Erlaubnistatbestand des § 28 BDSG ist einzuschränken

J. Taeger
Uni Oldenburg

Konfigurierbare und eingebettete Sicherheit • Leitung: N. Pohlmann

B

11.10 Uhr Konfigurierbare Sicherheit für Java Laufzeitumgebungen

- Sichere Java Laufzeitumgebung
- Konfigurierbare Verschlüsselung
- Wrapping von Klassen
- Anwendungsbeispiel Remote Method Invocation
- Durchsetzung von Policies

D. Peters
V. Gruhn
Uni Leipzig
T. Bühren
Peperoni GmbH

11.35 Uhr Seitenkanal Angriffe auf javabasierte Softwarearchitekturen

- Java und javabasierte Softwarearchitekturen
- System-Sicherheits-Mechanismen in J2SE/J2EE
- Side- und Covert-Channels
- Aktuelle Beispiele
- Entfernung der Anti-Patterns durch Refactoring

M. Schoenefeld
GADeG

12.00 Uhr Eingebettete Sicherheit – State-of-the-art

- Pervasive Computing und IT-Sicherheit
- Kryptographie im Automobil
- Protokolle für ad-hoc Netze
- Seitenkanalattacken
- Kryptomechanismen bei beschränkten Ressourcen

C. Paar
J. Pelzl
K. Schramm
A. Weimerskirch
T. Wollinger
Ruhr-Universität Bochum

12.25 Uhr Gemeinsame Mittagspause

Identitätsmanagement • Leitung: K. Keus

13.25 Uhr Benutzer und Berechtigungen – Modell zur Definition und Gestaltung

- Identity Management – zur begrifflichen Klarheit
- Motivation für einen ganzheitlichen Ansatz
- Abgrenzung zu bisherigen Vorgehensmodellen
- Beschreibung des Modells
- Perspektiven: Konsolidierung und Automatisierung

R. Holtkämper
Avinci AG

13.50 Uhr Identity Management – Infrastrukturaufgabe mit messbarem Nutzen

- Kosteneinsparung bei Benutzeradministration, Revision, Help Desk
- Produktivitätseffekte für den IT-Benutzer
- Höheres Sicherheitsniveau und dessen Bewertung
- Implementationskosten
- Modellrechnung für den Return on Investment

A. Kern
M. Kuhlmann
Beta Systems
Software AG

Mittwoch • 31. März 2004

14.15 Uhr Identity Management – Kosten und Nutzen

- Vorstellung eines praxisorientierten Modells zur Rol-Rechnung
- Planungssicherheit bei der Konzeption
- Nutzung eines produktunabhängigen Administrationsmodells
- Kosten- und Nutzenbetrachtung
- Aussagen zur optimalen Projektumsetzung durch Rol-Tool

M. Vogel
secunet AG

14.40 Uhr Kommunikationspause

Sicherheit als Strategie • Leitung: S. Paulus

15.10 Uhr IT-Security als Erfolgsfaktor in überbetrieblichen Wissensnetzwerken

- Wissensintensive Geschäftsprozesse
- Überbetriebliches Wissensmanagement
- Informationsaustausch und IT-Sicherheit in Wertschöpfungsnetzwerken
- Anforderungen an ein IT-Sicherheitskonzept
- Anwendungsbeispiel

S. Bleck
P. Laing
T. Scherle
RWTH Aachen

15.35 Uhr IT-Sicherheit und Basel II

- Basel II und IT-Sicherheit
- Messansätze
- Operationelle Risiken und BIA
- Kosten-Nutzen-Erwägungen
- IT und Operational Risk

R. von Rössing
Ernst & Young
Österreich

16.00 Uhr Lösen TCPA und Palladium die Sicherheitsprobleme von heute?

- TCG und NGSCB
- Aktuelle Sicherheitsprobleme
- Beispiel Wurm W32/Lovesan
- Wirkung vertrauenswürdiger Hardwaremodule
- Architektur und Grenzen vertrauenswürdiger Plattformen

A. Buchmann
F. Dötzer
H. Görl
S. Lachmund
TU-München

16.25 Uhr Konferenzende

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

- **Rollenbasierte Zugriffskontrolle im WebSphere Portal**
D. Buehler IBM Böblingen
- **Evaluierung von Angriffen auf steganographische Verfahren für JPEG-Bilder**
J. Dittmann • **A. Lang** Uni Magdeburg **A. Herrn** HWTH Leipzig
- **Return on Security Investment – die große Unbekannte**
F. Rustemeyer secunet AG
- **Implementierung des AES auf einer Smartcard und Seitenkanal-Attacken**
C. Paar • **K. Schramm** Ruhr-Universität Bochum
- **Partielle Verschlüsselung von MPEG Audio zum effizienten Schutz von Authentizität und Integrität**
M. Steinebach • **S. Zmudzinski** Fraunhofer IPSI

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

Programmkomitee

P. Horster Uni Klagenfurt (Vorsitz) • **J. Bizer** Uni Frankfurt • **J. Buchmann** TU Darmstadt • **C. Busch** FhG-IGD
W. Dettling FHBB Basel • **J. Dittmann** Uni Magdeburg • **C. Eckert** TU Darmstadt • **B. Esslinger** Deutsche Bank
T. Faber secure-it.nrw • **H. Federrath** Uni Regensburg • **D. Fox** Secorvo • **P. Gygax** IT KT. Basel-Stadt
R. Haefelfinger FI FGSec • **S. Janisch** Uni Salzburg • **D. Jäpel** IBM CH • **K. Keus** BSI • **P. Kraaibeek** secunet
W. Kühnhauser Uni Ilmenau • **P.J. Kunz** DaimlerChrysler • **I. Münch** BSI • **J. Nedon** ConSecur • **C. Paar** Uni Bochum
S. Paulus SAP • **G. Pernul** Uni Regensburg • **N. Pohlmann** FH Gelsenkirchen • **R. Posch** TU Graz
K. Rannenber Uni Frankfurt • **H. Reimer** TeleTrusT • **A. Roßnagel** Uni GH Kassel • **C. Ruland** Uni GH Siegen
I. Schaumüller ITS Linz • **P. Schartner** Uni Klagenfurt • **J. Swoboda** TU München • **S. Teiwes** Ernst & Young CH
S. Teufel Uni Fribourg • **C. Tschudin** Uni Basel • **J. von Knop** Uni Düsseldorf • **G. Weck** Infodas
M. Welsch IBM D • **P. Wohlmacher** RegTP • **K.-D. Wolfenstetter** T-Systems

Organisation

P. Kraaibeek secunet • **D. Cechak** Uni Klagenfurt • **C. Tschudin** Uni Basel



Anmeldung & Teilnahmebedingungen

D·A·CH Security 2004

30. und 31. März 2004

Universität Basel



via Fax an: ++49 (0)5921-722-493

oder Online-Formular unter: http://syssec.uni-klu.ac.at/DACH2004/index_anmeldung.html oder an:

Organisationskomitee D·A·CH Security 2004

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 2004 am 30. und 31. März 2004 an der Universität Basel an.**
- Ich kann an der Tagung nicht teilnehmen, bestelle aber ein Exemplar des Tagungsbandes zum Preis von € 79. Bei Bestellung bis zum 15. Februar gilt der Subskriptionspreis von € 59.**

Teilnahmebedingungen

Bei Anmeldung bis zum 15. Februar 2004 beträgt die Teilnahmegebühr € 285 (Frühanmeldegebühr), anschließend € 330 jeweils zuzüglich der gesetzlichen MwSt.

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 8. März 2004 (Datum des Poststempels) wird eine Bearbeitungsgebühr von € 75 (inkl. MwSt.) erhoben. Nach dem 8. März 2004 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