



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

D·A·CH Security

Ruhr-Universität Bochum | 19. und 20. Mai 2009



Aktuelle Informationen: <http://www.syssec.at/DACHSecurity2009/>



Dienstag • 19. Mai 2009

08.30 Uhr Registrierung, Kaffee und Tee

09.25 Uhr Begrüßung und Überblick | P. Horster | J. Schwenk

IT Security Management • Leitung: J. Taeger

A

09.35 Uhr Zehn Thesen zur Entwicklung der Informationssicherheit

- Position: Treiber und Steuerungslogik im Business
- Dauerbrenner: Softwarequalität und verteilte Sicherheit
- Security Information Event Management und Informationsflusskontrolle
- Reserven: Prozessgestaltung und Reputation
- Spielräume: Industrialisierung der IT und die Autorität der Anwender

E. von Faber
T-Systems und
FH Brandenburg

10.00 Uhr Ontologiebasiertes IT Risikomanagement

- Security Ontology als maschinell interpretierbare Wissensbasis
- Automatisierte Bewertung von Bedrohungen und Schwachstellen
- Objektive Bestimmung von Bedrohungseintrittswahrscheinlichkeiten
- Risikobestimmung auf Basis existierender Geschäftsprozesse
- Interaktive Auswahl von effizienten Gegenmaßnahmenportfolios

S. Fenz
TU Wien
A. Ekelhart
T. Neubauer
Secure Business
Austria

10.25 Uhr Compliance – Die Vorstandspflicht zur Beherrschung von Rechtsrisiken

- Compliance als Managementpflicht
- Maßnahmen der Compliance-Organisation
- Bedeutung der IT-Infrastruktur für die Compliance-Organisation
- Möglichkeiten der IT-Unterstützung bei der Sicherstellung von Compliance
- Rechtliche Grenzen des IT-Einsatzes

B. Schmidt
Uni Oldenburg

10.50 Uhr Kommunikationspause

Data Leakage Prevention und Zugriffssteuerung • Leitung: H. Reimer

A

11.20 Uhr Data Leakage Prevention

- DLP: mehr als ein Buzzword
- Marktsituation und Gefährdungspotentiale
- DLP und Netzwerk-Forensik
- Unternehmensspezifische Securitykonzepte als Basis für DLP
- Praktikable Ansätze und Grenzen von DLP

A. M. Tietz
Defense AG

11.45 Uhr Analyse von Zugriffssteuerungssystemen

- Zugriffsschutz in IT-Systemen
- Verdeckte Informationsflusspotenziale diskreter Zugriffssteuerungssysteme
- Zugriffssteuerung und Informationsflüsse
- Informationsflussanalyse zum Finden von Miskonfigurationen
- Automatisierte Analyse von Unix-Zugriffsschutzsystemen

P. Amthor
A. Fischer
W. Kühnhauser
TU Illmenau

12.10 Uhr Einsatz externer Autorisierungsmodule in Business-Anwendungen

- Konzept zur Externalisierung der Autorisierung
- Anforderungen an externe Autorisierungsmodule
- Beispiel: Microsoft AuthorizationManager (AzMan)
- Abdeckung der Anforderungen durch AzMan
- Fazit und Ausblick

M. Hübner
O. Paustjan
WestLB AG

Sicherheitsrelevante Anwendungen • Leitung: J. Dittmann

B

11.20 Uhr Schutz elektronischer Messdaten in der Energiewirtschaft

- Messdaten werden heute meist digital erfasst, gespeichert und übertragen
- Zulassungsvoraussetzung bei vielen Messgeräten: Einsatz von Kryptographie
- Formal gefordert: Digitale Signaturen auf Messdaten und Firmware-Updates
- Konzepte auf hohem Sicherheitsniveau existieren bereits (z. B. SELMA)
- Aktuelle Projekte setzen Kryptographie direkt auf Embedded-Prozessoren um

T. Zeggel
cv cryptovision
gmbh

Dienstag • 19. Mai 2009

11.45 Uhr Instant Messaging Systeme als Plattform für elektronisches Wählen

- Instant Messaging Systeme als Applikationsplattformen
- Spontane Entscheidungsprozesse
- Verbindliche Kommunikation über IMS
- Sichere Authentifikation ohne PKI-Nutzung
- Verifikation über den Video-Kanal

A. Meletiadou
Uni Koblenz

12.10 Uhr Erstellen und Identifizieren individueller Logos

- Individuelle Wasserzeichen für Logos
- Verfolgbarkeit unerlaubter Dokumentenweitergabe
- Umsetzungsbeispiel Modifikation von Linienbreiten
- Anwendungsbeispiel Faxübertragung
- Robustheit gegen analoge Verbreitung

M. Steinebach
A. Ruppel
Fraunhofer SIT

12.35 Uhr Gemeinsame Mittagspause

Sicherheitsrichtlinien und Zertifizierung • Leitung: G. Welsch

A

13.35 Uhr Security Standards und Richtlinien für Web-Anwendungen

- Angriffsvektoren auf Web-Anwendungen
- Relevante BSI-Studien und Grundschutz-Bausteine
- ÖNORM A 7700 zur Zertifizierung von Web-Anwendungen
- Open Web Application Security Project (OWASP) Guide
- Vergleich der Vorgaben am Beispiel Eingabevalidierung

T. Kerbl
SEC Consult
Unternehmens-
beratung GmbH

14.00 Uhr Sicherheitstechnische Zertifizierung von DB-Installationen

- Sicherheit der Konfiguration und Umgebung eines DBMS
- Defense in Depth
- Gewinnung von Best Practices
- Flexible Umsetzung
- Evaluierung und Zertifizierung

O. Angyal
N. Tekampe
TÜV Informations-
technik GmbH
U. Greveler
FH Münster

14.25 Uhr Die Pflicht Risiken zu managen – Gründe der Finanzkrise

- Die Finanzkrise als Folge unzureichenden Kreditrisikomanagements
- Gesellschaftsrechtliche Anforderungen an das Risikomanagement
- Transparenz und Kontrolle
- Information-Security als Risikomanagementfaktor
- Sicherheitsrelevanz der Informationsintegrität

C. Jakob
Uni Oldenburg

Sicherheitsanalyse und Forensik • Leitung: K.-D. Wolfenstetter

B

13.35 Uhr Pauschalisierte Sicherheitsbetrachtungen in automotiven Systemen

- Bedeutung von IT-Sicherheitsanforderungen für das Automobil
- Objekt-bezogene Gefährdungsanalyse angelehnt an BSI Grundschutz
- Modellierung von sicherheitsrelevanten/-kritischen Beziehungen
- Formale Beschreibung von logischen Zusammenhängen
- Semi-automatische Bestimmung von Sicherheitsanforderungen

S. Schulze
T. Hoppe
J. Dittmann
Uni Magdeburg

14.00 Uhr Forensische Datenarten und -analysen in automotiven Systemen

- Besonderheiten der Informationsverarbeitung in automotiven IT-Systemen
- Einsatzfeld der IT-Forensik als Hilfsmittel in der Unfallrekonstruktion
- Umsetzung der forensischen Maßnahmen im automotiven Systemumfeld
- Beschreibung des methodischen Ablaufs
- Vorstellung einer exemplarischen Untersuchung auf einer embedded MCU

S. Kiltz
M. Hildebrandt
J. Dittmann
Uni Magdeburg

14.25 Uhr Service-Fingerprinting mittels Fuzzing

- Service-Fingerprinting – Ein Kernpunkt effektiver Penetrationstests
- Bestehende Verfahren und deren Schwächen
- Service-Fingerprints einfach und automatisch erzeugen
- Praxistaugliche Implementierung eines Fuzzing-basierten Fingerprintings
- Erzielte Verbesserungen und Vergleich mit anderen Tools

S. Vandersee
S. Schemmer
rt-solutions.de GmbH
M. Hanspach
R. Schuhmann
FHDW Berg. Gladbach

14.50 Uhr Kommunikationspause



Dienstag • 19. Mai 2009

Schutz personenbezogener Daten • Leitung: P. Frießem

A

15.20 Uhr Irreversibler Verschluss: DRM-basierter Datenschutz

- Datenschutzfördernde Technologie auf Basis digitaler Rechteverwaltung
- Konzept des irreversiblen Verschlusses
- Nutzung von Trusted Computing
- Datenabgleiche, Datenpannen
- Anwendungsbeispiele der Technologie

U. Greveler
FH Münster

15.45 Uhr Massenpseudonymisierung von persönlichen medizinischen Daten

- Gefahren für den Datenschutz
- Operationen der Massenpseudonymisierung
- Hüllenbasiertes Sicherheitsmodell
- Sekundärnutzung medizinischer Daten
- Pseudonymisierung zur Verringerung datenschutzrechtlicher Bedenken

J. Heurix
TU Wien
T. Neubauer
Secure Business
Austria

16.10 Uhr Sichere Speicherung von Patientendaten mithilfe von Chipkarten

- Können Notfalldaten sicher auf Chipkarten gespeichert werden?
- Sichere Speicherung von Daten auf Chipkarten in nicht-erpressbarer Form
- Kryptographische Schwellwert-Verfahren zur Datenspeicherung
- Einsatz von Gesundheitskarten zum Notfallmanagement
- Effiziente und informationstheoretisch sichere Speicherung kritischer Daten

R. Wigoutschnigg
S. Rass
P. Schartner
Uni Klagenfurt

16.35 Uhr De-Mail und Co. – Hintergründe und Risiken der Bürgerportale

- De-Mail und Co. im Überblick
- Technische Details der einzelnen Komponenten
- Juristische Aspekte: Das Bürgerportalgesetz
- Offene Fragen in Recht und Technik
- Ausblick und Perspektiven

D. Werner
Kanzlei
Bergfeld & Partner
C. Wegener
Horst Görtz Institut
für IT-Sicherheit

Sicherheit als Managementaufgabe • Leitung: I. Münch

B

15.20 Uhr Business Resilience

- Zum Stand des Krisenmanagements
- Geänderte aufsichtliche Anforderungen
- Krisen und Versagen reaktiver Instrumente
- Krisenanfälligkeit und Business Resilience
- Business Resilience in der Unternehmenspraxis

R. v. Rössing
KPMG AG

15.45 Uhr Verfügbarkeit und Notfallplanung mit Hilfe der Visualisierung

- Gefahrenpotenziale auf einem Blick erschließen
- Zusammenhänge bei Anomalien besser erkennen
- Vorteile bei der Darstellung von Malware mit abstrakter Visualisierung
- Aktuelles Lagebild vom Ist-Zustand des Internets
- Overview first, then zoom and filter, and finally details on demand

S. Spooren
Institut für
Internet-Sicherheit

16.10 Uhr Management der Sicherheitsanforderungen

- Informationssicherheit und die dauerhafte Erfüllung von Anforderungen
- Kategorien von Anforderungen
- Der Anforderungsmanagement-Prozess als „Enabler“ eines ISMS
- Die Rolle des Anforderungsmanagers
- Ganzheitliche Unternehmens- und Behörden-Compliance mit System

A. Altrhein
P. Herrmann
A. Wiedemann
TÜV Informations-
technik GmbH

16.35 Uhr Security Reporting in großen Unternehmen

- Was man nicht messen kann, kann man nicht managen
- Messungen und Berichte im Management der Informationssicherheit
- Studie bei erfolgreichen Unternehmen
- Aktuell bestehende Lösungsansätze
- Ansätze für zukünftige Entwicklungen

G. Schimpf
smf team
H. Röckle
FH Ludwigshafen

17.00 Uhr Ende erster Konferenztag

19.30 Uhr Gemeinsames Abendessen

09.00 Uhr Authentisierungsverfahren für eGovernment-Dienste in Europa

- Authentisierung und Identifikation mit eID-Karten
- Authentisierungsdimensionen (Faktoren, Protokolle, Digitale Ausweise)
- Die EU-Landkarte der eID-Karten-Programme
- Eine Taxonomie elektronischer Dienste
- Der ePA in der internationalen Perspektive

D. Hühnlein

secunet AG

D. Houdeau

Infineon

Technologies AG

09.25 Uhr Ausländische Identitäten im österreichischen E-Government

- Identifikation im österreichischen E-Government
- Integration ausländischer Identitäten
- Analyse des Problems
- Entwicklung eines Konzepts
- Umsetzung mit Hilfe eines Demonstrators

K. Stranacher**T. Rössler****A. Tauber**

TU Graz

09.50 Uhr Langfristig beweiskräftige Signaturen mit dem eCard-API-Framework

- Das eCard-API-Framework gemäß BSI TR 03112
- Die Signaturfunktionen des eCard-API-Frameworks
- Beispielhafte Einsatzszenarien der elektronischen Signatur
- Vertrauenswürdige Langzeitarchivierung gemäß BSI TR 03125
- Realisierung der Referenzarchitektur mit der eCard-API

D. Hühnlein

secunet AG

U. Korte**U. Gnaida**

BSI

10.15 Uhr Quo vadis, Smartcard-Middleware?

- Es gibt eine Vielzahl von Krypto-Schnittstellen für Smartcards
- Nach PKCS#11 und MS-CAPI kommen CNG, ISO/IEC 24727 und andere
- Abbildung der Schnittstellen als Aufgabe der Smartcard-Middleware
- Steigende Komplexität erhöht die Bedeutung von Smartcard-Middleware
- Smartcard-Middleware als wichtiges Unterscheidungsmerkmal

K. Schmech**T. Mai****M. Hoffmeister**

cv cryptovision

gmbh

09.00 Uhr Das Horst Görtz Institut für IT-Sicherheit

- Geschichte: Von 0 auf 50 in 8 Jahren
- Lehre: Ein Bachelor und drei Master
- Absolventen: Von Wirtschaft bis Wissenschaft
- Forschung: Grundlagen und Anwendungsorientierung
- Workshops: Grundlagen bis Anwendungen

J. Schwenk**C. Wolf**

Uni Bochum

09.25 Uhr SOA Security – Web Services Standards und Angriffe

- Existierende Standards zur Sicherung von Web Services
- Was ist neu? Was ist besser?
- Anwendungsszenarien und Einsatzmöglichkeiten
- Standards vs. Realität. Ist sicher = sicher?
- Aktuelle Angriffe auf Web Services im Detail

M. Jensen**J. Schwenk**

Uni Bochum

09.50 Uhr Green Car Security: IT-Sicherheit und Elektromobilität

- Fahrzeuge mit Elektroantrieb: Potential und Stand der Technik
- EMobil-Infrastrukturen: Park&Charge-Systeme vs. Wechselakkusysteme
- Angriffspunkte in EMobil-Systemen (Batterien, Zahlungssysteme, etc.)
- Vertrauenswürdige Erfassung des Energieverbrauchs
- Anonymität in EMobil-Systemen (Location Privacy)

C. Paar**K. Schramm****A. Weimerskirch**

Uni Bochum

A. Rupp

Uni Massachusetts

10.15 Uhr Einsatz von Sicherheitskernen und Trusted Computing

- Übersicht Trusted Computing Funktionalitäten
- Kosteneffektive Sicherheit durch Virtualisierung
- Entwicklung moderner Sicherheitskerne (Beispiele: Turaya und OpenTC)
- Schutz privater Daten (Beispiel: Phishing)
- Anwendungen im Unternehmensumfeld (Festplattenverschlüsselung, VPN)

A. Sadeghi**M. Winandy**

Uni Bochum

10.40 Uhr Kommunikationspause



Mittwoch • 20. Mai 2009

Sichere Kommunikation in Netzwerken • Leitung: N. Pohlmann

A

- 11.10 Uhr Abhörsichere Mobilkommunikation mit IP- & ISDN-Telefonanlagen**
- Sicherheitsprobleme bei der Mobilkommunikation über GSM
 - Architektur einer sicheren, interoperablen Kommunikationslösung
 - Verschlüsselte Telefonkonferenzen
 - Integration in bestehende Telekommunikationsanlagen
 - Bewertung und Ausblick auf NGN, 2.5G und 3G

P. Backs
T. Korte
Sirrix AG

- 11.35 Uhr Beschreibung des Netzwerkverkehrs mittels Markow-Ketten**
- Überwachung des Netzwerkverkehrs
 - Statistische Beschreibung
 - Markow-Ketten
 - Parameterreduzierung
 - Anomalieerkennung

S. Bastke
Institut für
Internet-Sicherheit

- 12.00 Uhr Cisco Group Encrypted Transport VPN – Eine kritische Analyse**
- Motivation automatischer Konfiguration von IPsec-Infrastrukturen
 - Anforderungen an sichere Konfiguration solcher Infrastrukturen
 - Vorstellung Group Encrypted Transport VPN
 - Sicherheitsanalyse des Verfahrens
 - Ableiten von Richtlinien für einen sicheren Einsatz

M. Roßberg
G. Schaefer
TU Ilmenau

Schadsoftware und Angriffe • Leitung: W. Kühnhauser

B

- 11.10 Uhr Automatisierte Signaturgenerierung für Malware-Stämme**
- Herausforderungen und Probleme bei der Erkennung von Malware
 - Struktureller Vergleich von Malware über Aufruf- und Kontrollflussgraphen
 - Eine Heuristik für das k-LCS Problem
 - Automatische Generierung von Erkennungssignaturen für Malware-Stämme
 - Evaluierung der generierten Signaturen in Bezug auf False-Positives

C. Blichmann
TU-Dortmund

- 11.35 Uhr Onlinedurchsuchung versus Virens Scanner – Eine Aufwandsabschätzung**
- Verdeckter Eingriff in informationstechnische Systeme
 - Digitale Forensik und Remote Forensic Software (RFS)
 - Umgehbarkeit von Virens Scannern und Personal Firewalls
 - Weitere technische Zugriffsmöglichkeiten für die Online-Durchsuchung
 - Möglichkeit des einmaligen Einsatzes eines RFS, Aufwandsabschätzung

U. Greveler
C. Puls
FH Münster

- 12.00 Uhr Statistische Schadcodedetektion in ausführbaren Dateien**
- Statistische Schadcodeerkennung ausführbarer Windows-Binaries
 - Heuristischer Detektionsansatz für schwellwertbasierte statische Analyse
 - Vorstellung einer Analyse von 23 Attributen auf über 30.000 Testdateien
 - Bewertung der Testergebnisse und Vergleich mit kommerziellen Lösungen
 - Diskussion von Einsatz-Szenarien

T. Hoppe
R. Merkel
C. Krätzer
J. Dittmann
Uni Magdeburg

12.25 Uhr Gemeinsame Mittagspause

Digitale Signaturen und Biometrie • Leitung: U. Korte

A

- 13.25 Uhr Einfache, wirtschaftlich sichere Signaturen**
- Nur wirtschaftlich relevante Daten signieren
 - Beispiel: FinTS-Transaktionen
 - Vertrauenswürdige Signaturumgebung
 - Einfachheit: Nürnberger Sicherheitstrichter
 - Prototypische Implementierung

P. Trommler
S. Hehn
M. Brittig
Ohm-Hochschule
Nürnberg

- 13.50 Uhr Spezielle Signaturvarianten und Anwendungsbereiche**
- Erweiterungen digitaler (Standard)Signaturen
 - Multi-Dokument- und Multi-Signator-Signaturen
 - Gruppen-, Ring- und Blinde-Signaturen
 - Anwendungsszenarien im Unternehmensbereich
 - Nur Theorie – praktisch einsetzbar?

D. Slamanig
C. Stingl
FH Kärnten

Mittwoch • 20. Mai 2009

14.15 Uhr **Secure Sketches für biometrische Handschrift**

- Anwendungen von biometrischen Kryptosystemen
- Dynamische Handschrift als biometrisches Merkmal
- Variabilität biometrischer Daten
- Biometrische Hash-Funktionen und Secure Sketches
- Exemplarische Evaluierung

T. Scheidat
C. Vielhauer
M. Schott
Uni Magdeburg

Identitätsmanagement und Identitätsdiebstahl • Leitung: H. Storck

B

13.25 Uhr **User-Centric Identity Management in mobilen Szenarien im SIMOIT-Projekt**

- IT-Sicherheitsfaktoren
- Benutzerzentriertes Identity Management
- Lösungen für Endpunkt-Sicherheit
- Der SIMOIT-Ansatz auf Basis von TNC
- Sicherheitsmechanismen der eingesetzten Quarantänezone

K.-O. Detken
DECOIT GmbH

13.50 Uhr **Identity Management (IdM) in flexiblen Organisationen**

- IdM-Herausforderungen in flexiblen Organisationen
- Fallstudie für flexibles IdM
- Kritische Erfolgsfaktoren bei der IdM-Harmonisierung
- Mehrstufiger Integrationsprozess
- Technologische Lösungsansätze mittels Identity Federation

J. Wiedemann
O. Carr
M. Reil
Accenture GmbH

14.15 Uhr **Automatisierter Identitätsdiebstahl in sozialen Netzwerken**

- Hohes Angriffs-/Schadenspotenzial in sozialen Netzen
- Formale Beschreibung der Struktur sozialer Netze
- Datenaggregation und Datenkorrelation
- Automatisierte Angriffe mit optimaler Opferwahl
- Kommunikation der Kritikalität als Schutzmechanismus

D. Birk
F. Gröbert
C. Wegener
Horst Görzt Institut
für IT-Sicherheit

14.40 Uhr **Kommunikationspause**

Sichere Langzeitarchivierung • Leitung: A. Philipp

A

15.10 Uhr **Langzeitarchivierung: Verlust von Sicherheitseigenschaften der Hashfunktion**

- Anforderungen aus dem Signaturgesetz
- Verlust von Sicherheitseigenschaften des Signaturalgorithmus
- Verlust von Sicherheitseigenschaften der Hashfunktion
- Kryptographischer Hintergrund
- Lösungsvorschlag

W. Schindler
T. Biere
BSI

15.35 Uhr **Technische Richtlinie zur vertrauenswürdigen Langzeitarchivierung**

- Anforderungen an vertrauenswürdige elektronische Langzeitarchivierung
- Produktunabhängige Architektur und standardbasierte Schnittstellen
- Anwendungsneutrale Definition der Prozesse
- Empfehlungen für Daten und Langzeitspeicherformate
- Zertifizierbarkeit auf Basis dieser technischen Richtlinie

P. Rehäuser
W. Zimmer
CSC GmbH
U. Korte
S. Fischer-Dieskau
BSI

16.00 Uhr **Migration zur Langzeitarchivierung von elektronischen Textdokumenten**

- Migration von Textdokumenten zur digitalen Langzeitarchivierung
- Problem von Informationsverlusten bei Migration
- Utility Analysis zur Erstellung eines strukturierten Kriterienkatalogs
- Beurteilung und Wichtung von Einzelkriterien
- Fallstudie: AmiPro-Dateien nach OOXML, ODF und PDF/A

J. Adelmeier
C. Vielhauer
FH Brandenburg
M. Schott
Uni Magdeburg

16.25 Uhr **Konferenzende**

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

- **Nutzung von Sozialen Netzwerk-Plattformen für die Verteilung von Public Keys**
M. Hülber, V. Wolff-Marting Uni Leipzig
- **Föderation von PKI-Repositories**
G. Jacobson Secardeo GmbH

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



Anmeldung & Teilnahmebedingungen

D•A•CH Security 2009
19. und 20. Mai 2009
Ruhr-Universität Bochum



hgi
Horst Görz Institut
für IT-Sicherheit

Anmeldung zur Konferenz

Online-Anmeldung unter: http://www.syssec.at/ds09_anmeldung/

Unter dieser Adresse kann auch ein ausdrucksbares Anmeldeformular herunter geladen werden.

Teilnahmebedingungen

Bei Anmeldung bis zum 26. April 2009 beträgt die Frühmeldegebühr € 335.– zzgl. MwSt. (€ 398,65) bei Anmeldung ab 27. April 2009 beträgt die Teilnahmegebühr € 420.– zzgl. MwSt. (€ 499,80).

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 22. April 2009 (Datum des Poststempels) wird eine Bearbeitungsgebühr von € 75.– (inkl. MwSt.) erhoben. Nach dem 22. April 2009 ist die volle Tagungsgebühr zu entrichten. Es ist jederzeit die Benennung einer Ersatzperson ohne zusätzliche Kosten möglich.

Zusätzliche Tagungsbände

Zusätzliche Tagungsbände können bestellt werden unter:
<http://www.syssec.at/tagungsbaende/>

Organisationskomitee

Organisationskomitee D•A•CH Security 2009

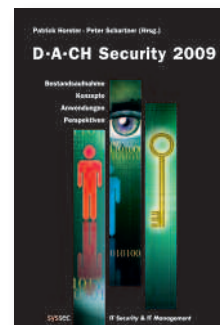
Peter Kraaibeek

Bogenstr. 5a

D-48529 Nordhorn

Telefon: ++49 (0)5921-722-490

E-Mail: Peter@Kraaibeek.com



Programmkomitee:

P. Horster Uni Klagenfurt (Vorsitz) • **R. Ackermann** SAP • **C. Busch** Fraunhofer IGD

J. Dittmann Uni Magdeburg • **P. Frießem** Fraunhofer SIT • **M. Hartmann** SAP

E. Haselsteiner NXP Semiconductors • **D. Hattenberger** Uni Klagenfurt • **S. Janisch** Uni Salzburg

D. Jäpel IBM CH • **T. Kob** HiSolutions • **F. Kollmann** BearingPoint • **U. Korte** BSI • **P. Kraaibeek** secunet

W. Kühnhauser Uni Ilmenau • **P.J. Kunz** Daimler • **S. Lechner** JRC • **H. Leitold** A-SIT • **I. Münch** BSI

L. Neugebauer BITKOM • **A. Philipp** Utimaco • **N. Pohlmann** FH Gelsenkirchen • **R. Posch** TU Graz

H. Reimer TeleTrusT • **A. Roßnagel** Uni GH Kassel • **W. Schäfer** DATEV • **M. Schaffer** NXP Semiconductors

P. Schartner Uni Klagenfurt • **D. Sommer** IBM Research • **H. Storck** Nokia Siemens Networks

J. Taeger Uni Oldenburg • **S. Teufel** Uni Fribourg • **G. Weck** Infodas • **C. Wegener** Uni Bochum

G. Welsch TeleTrusT • **K.-D. Wolfenstetter** DTAG

Organisation:

D. Cechak Uni Klagenfurt • **P. Kraaibeek** secunet • **V. Hintzmann** Uni Bochum