OESTERREICHISCHE COMPUTER GESELLSCHAFT
AUSTRIAN COMPUTER SOCIETY

TeleTrusT
Pioneers in IT security.

Gemeinsame Arbeitskonferenz: GI | OCG | TeleTrusT

D·A·CH Security

Universität der Bundeswehr München
5. und 6. September 2017

Aktuelle Informationen: http://www.syssec.at/dachsecurity2017

infodas
Cologne IT Solutions & Services

syssec
Alpen-Adria-Universität Klagenfurt
System Security Group

Universität der Bundeswehr München

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

AFCEA Bonn e.V.

ESG

SANS EMEA
WWW.SANS.ORG

itsa 2017
Die IT-Security Messe und Kongress
The IT Security Expo and Congress

Bundesministerium des Innern

Dienstag • 5. September 2017

08.30 Uhr **Registrierung, Kaffee und Tee**

09.30 Uhr **Begrüßung und Überblick**

Security Awareness • Leitung: P. Schartner

09.35 Uhr **Security Awareness: Nicht nur schulen – überzeugen Sie!**

A. Schütz
K. Weber
FHWS

- Security Awareness: Komplexes Zusammenspiel verschiedener Faktoren
- Mitarbeitersensibilisierung muss Wissen, Wollen und Können fördern
- Integriertes Verhaltensmodell als Schlüssel zum Mitarbeiterverhalten
- Messung Security Awareness mit Hilfe verschiedener Faktoren
- Sensibilisierung durch individuelle Maßnahmen zur Verhaltensänderung

10.00 Uhr **Zur Wirksamkeit von Security-Awareness-Maßnahmen**

G. Schembre
A. Heinemann
Hochschule Darmstadt

- Social Engineering Angriffe erfordern Security Awareness
- Vergleich geeigneter Security-Awareness-Maßnahmen für ein KMU
- Untersuchung der Wirksamkeit im Rahmen einer empirischen Studie
- Durchführung unter praxisnahen und realitätsgetreuen Bedingungen
- Steigerung der Security Awareness bei E-Mail-Phishing-Angriffen

10.25 Uhr **Sozio-technische Aspekte von Finanz- und Cyberkriminalität**

R. Merkel
J. Dittmann
Uni Magdeburg
S. Reichmann
M. Griesbacher
Uni Graz

- Finanzkriminalität als herausforderndes interdisziplinäres Themenfeld
- Modi Operandi von Tätern
- Erkenntnisse auf Basis von Täterinterviews
- Potentielle Anknüpfungspunkte zur Stärkung von Cyber Security
- Gegenmaßnahmen auf technischer, psychologischer und soziologischer Ebene

10.50 Uhr **Kommunikationspause**

Audits, Penetration-Tests & Forensik • Leitung: E. Weippl A

11.20 Uhr **Security Audits von Embedded Systems mit Mikrocontrollern**

M. Kammerstetter
D. Burian
S. Riegler
Trustworks KG

- Viele Embedded Systems setzen auf günstige Standard-Mikrocontroller
- Firmware-Inhalte sind üblicherweise gegen das Auslesen geschützt
- Ohne Firmware-Extraktion ist kein tiefgehender Security-Test möglich
- Es werden Labormethoden zur Firmware-Extraktion und -Analyse vorgestellt
- Dadurch können enthaltene Schwachstellen identifiziert werden

11.45 Uhr **Evolutionäres unstrukturiertes Fuzzing von L4-Mikrokernen**

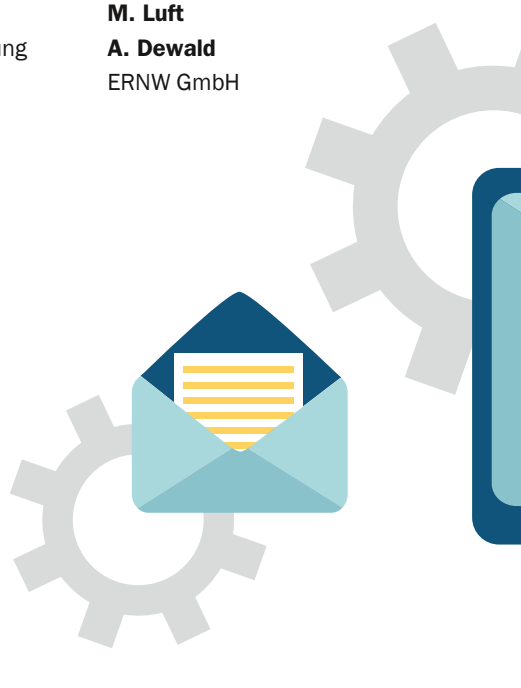
D. Loebenberger
genua GmbH
S. Liebergeld
Kernkonzept GmbH

- L4 Mikrokerne sind für die Sicherheit vieler IT-Systeme grundlegend
- „Fuzzing“ ist eine erfolgversprechende Methode für Penetrationtests
- Neuerdings ist es möglich, Fuzzing im laufenden Betrieb durchzuführen
- Damit können erstmals L4 Mikrokerne wie L4Re derart untersucht werden
- Die Ergebnisse erstaunen!

12.10 Uhr **Incident Analyse und Forensik in Docker-Umgebungen**

M. Luft
A. Dewald
ERNW GmbH

- Forensik und Incident-Analysen aufgrund Cybercrime an der Tagesordnung
- Steigender Einsatz von Docker im Unternehmensumfeld
- Auswirkungen auf forensische Untersuchungen unklar
- Welche Änderungen ergeben sich für Spuren, Methoden und Prozesse?
- Welche neuen Spuren entstehen durch Docker selbst?



Dienstag • 5. September 2017

Identifikation & Privatsphäre • Leitung: M. Ullmann — B

11.20 Uhr **Design- und Implementierungsaspekte mobiler abgeleiteter Identitäten**
- Mobile Geräte eignen sich gut als zweiter Faktor bei der Authentisierung
- Überblick über europäische Systeme für abgeleitete IDs im eGovernment
- Speicherorte für mobile abgeleitete Identitäten
- Registrierungsprozeduren für mobile abgeleitete Identitäten
- Designaspekte zur Zugriffsabsicherung auf abgeleitete Identitäten

D. Träder
A. Zeier
A. Heinemann
HS Darmstadt

11.45 Uhr **Migration von OpenID Connect in eine bestehende Anwendungslandschaft**
- Einführung in OpenID Connect
- Konzeptionelle Einordnung einer Migration
- Wege zur Migration
- Demonstration an Praxisbeispielen
- Erfahrungsbericht (Lessons Learned)

R. H. Steinegger
S. Abeck
Karlsruher Institut für Technologie
A. Hotz, N. Hintz
iC Consult

12.10 Uhr **PET-unterstützte Freigabeverfahren für offene Daten**
- Offene Daten in der öffentlichen Verwaltung
- Prinzip: open by default, Ausnahme: Personenbezug
- PET-unterstützte automatisierte Freigabeverfahren
- Betrachtung: False Positives/Negatives
- Kritische Diskussion der Wirksamkeit

U. Greveler
HS Rhein-Waal

12.35 Uhr **Gemeinsame Mittagspause**

IT Monitoring • Leitung: W. Rankl — A

13.35 Uhr **Softwaredesign für Dynamische Integritätsmessungen bei Linux**
- Dynamische Integritätsmessungen eines Linuxsystems zur Laufzeit
- Integritätskonzept mit Hilfe von Trusted Computing Ansätzen
- Vorberechnung statischer Referenzwerte für Prozesse
- Dynamische Nachberechnung von Kernelmodifikationen in der Verifikation
- Analyse des Einflusses der Integritätsmessungen auf die Systemleistung

M. Jahnke, T. Rix, K.-O. Detken
DECOIT GmbH
A. Rein
Huawei Technologies

14.00 Uhr **Security-Monitoring beim Pairing in Wireless Sensor Networks**
- Wireless Sensor Networks im Internet of Things
- Restriktionen bei Stromverbrauch und Rechenleistung der IoT Devices
- Sicherheits-Risiken in Wireless Sensor Networks
- Übersicht zu Angriffen und Gegenmaßnahmen
- Erkennung von Angriffen in der Pairing-Phase von neuen Devices

O. Krebs
I. Schiering
T. Lorenz
Ostfalia HAW
A. Hitzmann
Osaka University

14.25 Uhr **Cyber Range: Netzverteidigung trainieren mittels Simulation**
- Effiziente Angriffserkennung und -bewältigung als Herausforderung
- Eklatanter Bedarf: Gut ausgebildetes Personal im Cyber-Umfeld
- Simulation als ideales Mittel zum Testen & Üben von Handlungsabläufen
- Cyber Range-Einsatz in operativem Training und universitärer Lehre
- Wesentliche Anforderungen und Aufbau einer Cyber Range

R. Kaschow
O. Hanka
ESG
M. Knüpfer
V. Eiseler
UniBw München

Dienstag • 5. September 2017

Studentische Abschlussarbeiten • Leitung: S. Schauer — B

13.35 Uhr **Security Awareness auf Basis von Open Educational Resources** — **J. J. Tschöll**, HS Furtwangen
- Grenzen des Urheberrechts in der Security Awareness
- Der „Open-Source-Ansatz“ im Non-Software-Bereich
- Chancen für Security Awareness durch OER
- Gewährleistung der Auffindbarkeit von OER
- Qualitätssicherung und Finanzierung offener Materialien

14.00 Uhr **Entwicklung einer Benchmark Software für kryptografische Hashfunktionen** — **M. Schlüchter**, FH-Dortmund
- Erläuterung der Funktionsweise aktueller kryptografischer Hashfunktionen
- Vorstellung bestehender Implementierungen und Softwarelösungen
- Aufbau, Konzepte und Softwarearchitektur der Eigenimplementierung
- Besonderheiten bzgl. der Teststrategie bei kryptografischen Hashfunktionen
- Fazit und Evaluation der Implementierung

14.25 Uhr **IoT Architektur zum Schutz von Privatsphäre Ende-zu-Ende** — **S. Funke**, TU Darmstadt
- Bedrohungsmodell der Privatsphäre für das Internet der Dinge (IoT)
- Kompositorisches Privacy Enhancing Technology (PET) Taxonomiemodell
- Privatsphären-Schutz Metrik für komponierte PET Systeme
- Kontext-sensitive Privatsphäre Architektur für IoT Infrastrukturen
- Prototyp Implementierung und Evaluation am Beispiel Fitness-Tracking

14.50 Uhr Kommunikationspause

Kritische Infrastrukturen • Leitung: I. Münch — A

15.20 Uhr **Monitor IT-Sicherheit kritischer Infrastrukturen** — **S. Dännart**, **T. Gurschler**, **U. Lechner**, UniBw München
- IT-Sicherheit in kritischen Infrastrukturen
- Aspekte nationaler und internationaler IT-Sicherheitsstudien
- Die Bedrohungslage in deutschen Unternehmen
- Realisierung von IT-Sicherheit in Deutschland
- Bedarf nach Forschungsergebnissen und neuen Technologien

15.45 Uhr **Moderne Energieverteilnetze: Bedrohungen und Gegenmaßnahmen** — **C.-H. Genzel**, **O. Hoffmann**, **R. Sethmann**, HS Bremen
- Einführung zum Energienetz und zukünftigen Energieverteilnetzen
- Bedrohungsanalyse für dezentrale Standorte im Energieverteilnetz
- Vorstellung relevanter Informationssicherheitsstandards im Energienetz
- Empfehlungen für Sicherheitsmaßnahmen im Energieverteilnetz
- Aufforderung zu mehr proaktiver Informationssicherheit im Energienetz

16.10 Uhr **Security-Self-Assessment in kritischen Infrastrukturen** — **J. Schneider, D. Fuhr**, HiSolutions AG, **E. Korte**, Pretherm GmbH, **C. Thim**, Universität Potsdam
- Wasserinfrastrukturen besitzen ein besonderes KRITIS-Risikoprofil
- Dies stellt insbesondere kleinere Betreiber vor Herausforderungen
- Im Forschungsprojekt Aqua-IT-Lab wurde ein Self-Assessment entwickelt
- Dieses erstellt aufwandsarm und selbsterklärend ein Risikoprofil
- Und generiert automatisch priorisierte Handlungsempfehlungen

16.35 Uhr **Artificial Intelligence to Predict Malicious Infrastructure** — **S. Truvé**, **G. Beeker**, Recorded Future
- IT Security ist bekannten Angriffen immer einen Schritt hinterher
- Prädiktive Informationen machen Verteidiger proaktiv statt reaktiv
- Historische und aktuelle Daten werden zu Bedrohungsinformationen
- Die Vorhersage von bösartiger Infrastruktur ist möglich geworden
- Mit Machine Learning zukünftige bösartige IP-Adressen Vorhersagen

17.00 Uhr Ende erster Konferenztag

18.30 Uhr Gemeinsames Abendessen

Mittwoch • 6. September 2017

Risikomanagement • Leitung: D. Pawelczak — A

09.00 Uhr **High-Level Risikoanalyse im Bereich Internet of Things** — **S. Schauer**
- Strukturierung von IoT-Domänen und Anwendungsfällen — **S. König**
- Security-Charakteristika von IoT-Systemen — **M. Latzenhofer**
- Identifikation von generischen Risiken — **S. Schiebeck**
- Vorschlag für eine High-Level IoT-Risikomatrix — AIT
- Konzeptionelle Handlungsvorschläge zur Risikominimierung

09.25 Uhr **Subjektive Risikobewertung – über Datenerhebung und Opinion Pooling** — **J. Wachter**
- Opinion Pooling — **S. Rass**
- Empirische Erhebung von Risikodaten — AAU Klagenfurt
- Risikodatenbereinigung — **S. Schauer**
- Risikodaten-Aggregation (verlustfrei und verlustbehaftet) — **S. König**
- Anwendungen im Risikomanagement — AIT

09.50 Uhr **Risikominimierung bei kommerziell genutzter Open Source** — **H. Fleischhauer**
- Schwachstellenerkennung im Software-Entwicklungsprozess — Hensoldt Sensors GmbH
- Eignung der Verfahren zum Monitoring und zur Risikobehandlung — **S. Haßdenteufel**
- Sicherheitslücken als Sachmangel — SSW Schneider Schiffer Weihermüller
- Haftung von Softwareherstellern
- Wirksamkeit von Haftungs- und Gewährleistungsausschlüssen

10.15 Uhr **Erstellung eines detaillierten Risikobehandlungsplans** — **H. Rudolph**
- Detaillierte Maßnahmenplanung aus dem Risikomanagement — **S. Giebelhausen**
- Risikobehandlungspläne als Kern des Risikomanagements — **M. Müller**
- Technische und organisatorische Maßnahmenbündel über alle ISMS-Level — admeritia GmbH
- Workshop-basierte Vorgehensweise
- Abstimmung der Maßnahmen auf ihre Betriebsverträglichkeit

SECMGT Workshop • Leitung: D. Koschützki — B

09.00 Uhr **Virtuelle Räuber, falsche Präsidenten und echte Erpresser** — **C. Hesse**
- Die Zahl komplexer IT-Angriffe nimmt weltweit zu — Riskworkers GmbH
- Manipulation mittels Social Engineering ist dabei essentiell
- Gegenmaßnahme ist eine adäquate Awareness-Strategie
- Allein einfache Standard-Maßnahmen anzuwenden, ist wenig hilfreich
- Awareness sollte auf Risiken & Mitarbeiter zugeschnitten sein

09.50 Uhr **IT-Sicherheit für kritische Infrastrukturen** — **S. Rudel**
- Durchführung von Vernetzung und Wissenstransfer der Verbundprojekte — UniBw München
- Begleitende Forschung zur Lage der IT-Sicherheit im Themenfeld — **M. Rass**
- Entwicklung von Methoden zu Open Innovation und IT-Security Matchplays — **M. Jalowski**
- Rechtliche Begleitung und Fachgruppen zur Normung und Standardisierung — FAU Erlangen-Nürnberg
- Zusammenführen von Good Practices von Betreibern kritischer Infrastrukturen

10.40 Uhr **Kommunikationspause**

Mittwoch • 6. September 2017

Richtlinien, Beweiswert & Datenschutzrecht • Leitung: K. Knorr — A

11.10 Uhr **Auf dem Weg zur Umsetzung der PSD2-Richtlinie** — **D. Hühnlein et al.**, ecsec GmbH

- Relevanz der Richtlinie (EU) 2015/2366 („Payment Services Directive 2“)
- Wesentliche Anforderungen der Richtlinie (Authentisierung, Kontozugriff...)
- Optionen für eine sichere PSD2-Implementierung auf Basis von Standards
- Berührungspunkte und Synergien zwischen PSD2 und eIDAS
- Ausblick zur Implementierung und Standardisierung von PSD2

11.35 Uhr **Datenpakete zur Informations- und Beweiswerterhaltung – ein Vergleich** — **S. Schwalm et al.**, BearingPoint GmbH

- Beweiswerterhaltung, technische Lösungen in der Langzeitarchivierung
- RFC4998/6283, Evidence Records, BSI TR-03125 TR-ESOR, XAIP, XFDU
- eIDAS-VO, ETSI EN 319 162 Associated Signature Containers (ASiC)
- ISO19005-3, PDF/A-3
- Bewertung verschiedener Technologien und Ausblick

12.00 Uhr **Das neue Datenschutzrecht im Überblick** — **D. Nemmert**

- Überblick über das neue Datenschutzrecht in Europa — **D. Hühnlein**
- Einblick in Kernartikel der Datenschutz-Grundverordnung — **T. Hühnlein**
- Erste Analyse einer frühen Version der ePrivacy-Verordnung — **M. Rauh**
- Kommende Anpassungen für das Bundesdatenschutzgesetz — **S. Baszanowski**
- Umsetzung der Anforderungen am Beispiel „SkIDentity“ — ecsec GmbH

Technische Aspekte • Leitung: G. Jacobson — B

11.10 Uhr **Mikrokern für zulassungspflichtige Hochsicherheitssysteme** — **T. Günther**, INFODAS GmbH

- Netzübergänge dienen Sicherheitsdomänen-übergreifender Kommunikation
- Bei Verschlusssachen sind besondere Anforderungen zu berücksichtigen — **M. Hohmuth**
- Sichere Ablaufplattform ist eine Grundvoraussetzung — **A. Lackorzynski**
- Mikrokern ermöglicht formelle Evaluierung — **M. Lange**
- Separierung von Prozessen und Hardware kann nachgewiesen werden — Kernkonzept GmbH

11.35 Uhr **Angriffe auf RDP – wie man RDP-Sitzungen abhört** — **A. Vollmer**, SySS GmbH

- RDP dient der Fernadministration und ist nahezu omnipräsent
- Fast immer werden selbstsignierte SSL-Zertifikate eingesetzt
- Diese Standardeinstellung bietet keinerlei Abhörschutz
- Entwicklung eines Proof-of-Concepts in Python um Passwörter einzusehen
- Empfehlungen und Gegenmaßnahmen

12.00 Uhr **SSDs und Verschlüsselung: Datenremanenz als Problem** — **C.-D. Hailfinger**, **K. Lemke-Rust**, HS Bonn-Rhein-Sieg

- Flashspeicher in SSDs als nichtlinear adressiertes Medium
- Flash Translation Layer (FTL) als Hardwareabstraktionsschicht in SSDs
- Systembedingte Datenremanenz als Eigenschaft eines FTL
- Sicherheitsannahmen gängiger Datenträgerverschlüsselungslösungen (FDE)
- Schwachstellen in FDE auf SSDs

12.25 Uhr **Gemeinsame Mittagspause**

Mittwoch • 6. September 2017

Software-Sicherheit • Leitung: P. Horster A

13.25 Uhr **Formale Methoden als Werkzeug für Software Security**
P. Schwemmer
WIBOND Informationssysteme GmbH

- Schwachstellen-Analysen zu schwerwiegenden IT-Sicherheitsvorfällen
- Modellierung sicherheitsrelevanter Abläufe
- Betrachtung grundlegender, formaler Methoden zur Programmanalyse
- Verifikation sicherheitsrelevanter Abläufe mit TESLA
- Usable Security im Softwareentwicklungsprozess = Software Security

13.50 Uhr **Java Sicherheitsanalyse mit Pattern-Detection-Tools**
M. Kreitz
A. Baumann
UniBw München

- Tool-gestützte Bewertung der Sicherheit von Java-Programmen
- Eignung von Pattern-Detection-Tools im Bereich der sicheren Software
- Auffinden von sicherheitsrelevanten Schwachstellen in Java-Quelltexten
- Beschreibung von typischen Sicherheitslücken mit Hilfe von Mustern
- Vorstellung eines eigenen Tools an konkreten Beispielen

14.15 Uhr **Security in der Java-Grundausbildung**
A. Baumann
D. Pawelczak
UniBw München

- Defizite und aktueller Stand des Themas Security in der Ausbildung
- Analyse der Oracle „Secure Coding Guidelines for Java SE“
- Integration sicherheitsrelevanter Aspekte in die Java Grundausbildung
- Konkrete Programmierbeispiele im Hinblick auf sichere Software
- Diskussion der gewählten Lehrinhalte und möglicher Alternativen

14.40 Uhr Kommunikationspause

Automatisierung • Leitung: A. Baumann A

15.10 Uhr **Drahtloses Abhören von Bussystemen in der Gebäudeautomatisierung**
A. Attenberger
FH Kufstein

- Steigende Verbreitung von Bussystemen
- Smart Home mit einer Vielzahl von Sensoren, Aktoren
- Geringe technische Hürden zur Abhörung
- Vorstellung eines einfachen Systems ohne physische Eingriffe
- Analyse von Ritto Twinbus Datentelegrammen

15.35 Uhr **Fingerabdruck-Identifizierung im Seniorenwohnheim**
K. Knorr
A. Schmidt
Hochschule Trier
T. Wambach
Universität Koblenz

- Erfahrungsbericht Fingerabdruck-Identifizierung im Seniorenwohnheim
- Datenschutzaspekte der biometrischen Authentisierung
- Überprüfung der IT-Sicherheit durch Sicherheitsuntersuchung
- Schutzkonzept basierend auf dem BSI IT-Grundschutz
- Bedrohungsanalyse Minutien

16.00 Uhr **Safety nicht ohne Security in der kollaborativen Robotik**
B. Breiling
B. Dieber
B. Reiterer
A. Schlotzhauer
S. Taurer
Joanneum Research

- Safety in der kollaborativen Robotik
- Sichere Planung für Roboteranwendungen
- Angriffe auf das Robot Operating System
- Security im Robot Operating System
- Demonstration eines Angriffs auf Safety-Komponenten in einem Robotersystem

16.25 Uhr Konferenzende

… als Referenten haben sich zusätzlich zur Verfügung gestellt:

- **Integration von SDN in eine virtualisierte IT-Topologie**
  J. Sell FH Dortmund • **E. Eren** Hochschule Bremen
- **IT-Sicherheitsanalyse durch NAC-Systeme mit SIEM-Funktionalität**
  C. Kleiner, M. Rhode Hochschule Hannover • **K.-O. Detken** DECOIT GmbH • **M. Steiner** IT-Security(at)Work
- **Starke Authentisierung – jetzt!**
  D. Hühnlein et al. ecsec GmbH

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

Anmeldung & Teilnahmebedingungen

D·A·CH Security 2017

5. und 6. September 2017

Universität der Bundeswehr München

Anmeldung zur Konferenz

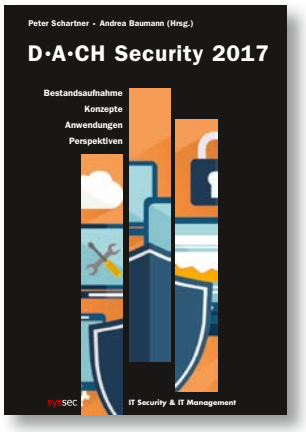
Telefon: +43 (0) 463 2700 3702
Online-Anmeldung unter:
http://www.syssec.at/ds17_anmeldung

Teilnahmebedingungen

Bei Anmeldung bis zum 14. August 2017 beträgt die Teilnahmegebühr € 395,- (Frühanmeldegebühr), danach € 480,- jeweils zuzüglich der gesetzlichen Mwst. Referenten zahlen nur die Referentengebühr von € 345,- zzgl. 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 14. August 2017 (Datum des Poststempels) wird eine Bearbeitungsgebühr von € 75,- erhoben. Nach dem 14. August 2017 ist die volle Tagungsgebühr zu entrichten. Es ist jederzeit die Benennung einer Ersatzperson ohne zusätzliche Kosten möglich.

Tagungsbände

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



Kontakt

Alpen-Adria-Universität Klagenfurt
Forschungsgruppe Systemsicherheit (syssec)
Universitätsstr. 65-67
A-9020 Klagenfurt
URL: http://www.syssec.at
E-Mail: konferenzen@syssec.at

Programmkomitee

Vorsitz: **P. Schartner** AAU Klagenfurt | **A. Baumann** UniBw München

P. Beenken Porsche AG • **J. Dittmann** Uni Magdeburg • **D. Engel** FH Salzburg • **F. Englberger** UniBw München
K. Frintrop AFCEA • **J. Fuß** FH Hagenberg • **H. Görl** UniBw München • **K.-P. Graf** UniBw München
M. Hartmann SAP • **P. Horster** AAU Klagenfurt • **D. Hühnlein** ecsec GmbH • **G. Jacobson** Secardeo GmbH
S. Janisch Uni Salzburg • **A. Kreth** AFCEA • **K. Knorr** HS Trier • **U. Korte** BSI • **W. Kühnhauser** TU Ilmenau
P.J. Kunz Daimler • **S. Lechner** JRC • **H. Leitold** A-SIT • **K. Lemke-Rust** HS Bonn-Rhein-Sieg • **M. Meier** Uni Bonn
B. Mester datenschutz nord • **H. Mühlbauer** TeleTrusT • **I. Münch** BSI • **J. Neuschwander** HTWG Konstanz
D. Pawelczak UniBw München • **A. Philipp** PrimeKey Labs GmbH • **N. Pohlmann** FH Gelsenkirchen
R. Posch TU Graz • **W. Rankl** Infineon Technologies AG • **S. Rass** AAU Klagenfurt • **A. Roßnagel** Uni GH Kassel
S. Schauer AIT • **H. Storck** T-Systems GmbH • **S. Teufel** Uni Fribourg • **P. Trommler** TH Nürnberg
M. Ullmann BSI • **G. Weck** Infodas • **C. Wegener** Uni Bochum • **E. Weippl** SBA Research • **S. Wendzel** HS Worms/FKIE
S. Werth BM des Inneren • **A. Wespi** IBM CH • **B.C. Witt** it.sec GmbH • **K.-D. Wolfenstetter** DTAG

GI-FG SECMGT Workshop

Leitung: **I. Münch** BSI • **B.C. Witt** it.sec GmbH • **D. Koschützki** HS Furtwangen

K. Kirst PTLV • **D. Koschützki** HS Furtwangen
P. Reymann ITQS • **J. Voßbein** UIMC

Organisation

A. Baumann UniBw München • **M. Möhlmann** • **B. Merl** AAU Klagenfurt • **P. Schartner** AAU Klagenfurt

Leitungsgremium der Konferenzreihe

P. Horster AAU Klagenfurt • **P. Schartner** AAU Klagenfurt