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

D·A·CH Security

Nürnberg | 17. und 18. September 2013

Aktuelle Informationen: http://www.syssec.at/dachsecurity2013

Bundesministerium des Innern

GEORG-SIMON-OHM HOCHSCHULE NÜRNBERG

itsa 2013 Die IT-Security Messe und Kongress The IT Security Expo and Congress

HISOLUTIONS

STONESOFT A McAfee Group Company

syssec

Dienstag • 17. September 2013

08.30 Uhr **Registrierung, Kaffee und Tee**
09.30 Uhr **Begrüßung und Überblick**

E-Card & E-Business • Leitung: K.-D. Wolfenstetter — A

09.35 Uhr **Elektronische Identität und Stellvertretung in Österreich** — **A. Tauber**, **B. Zwattendorfer**, **K. Stranacher**, EGIZ/TU Graz
- Österreichische Bürgerkarte
- Elektronische Stellvertretung und Vollmachten
- Das österreichische eID- und Stellvertretungs-Konzept
- Vertretung von natürlichen und juristischen Personen
- Online Vollmachten-Service

10.00 Uhr **Elektronische Signaturen mit der Open eCard App** — **D. Hühnlein**, **J. Schmölz**, **T. Wich**, ecsec GmbH, **A. Kühne**, Trustable Ltd
- Die Signatur ist tot – lang lebe die Signatur!
- Das Standard-basierte eCard-API-Framework
- Die Open eCard Plattform für eID, Signatur und mehr
- {C,X,P}AdES-Plugins für die Open eCard App
- Die „Open Signature Initiative“ lädt zur Mitwirkung ein!

10.25 Uhr **Redigierbare Signaturen in e-Business Anwendungen** — **K. Stranacher**, **B. Zwattendorfer**, TU Graz
- Konventionelle Signaturen erkennen Modifikationen der Daten
- Redigierbare Signaturen ermöglichen nachträgliche Änderungen
- Rechtliche und technische Anforderungen für Redigierbare Signaturen
- Evaluierung und Bewertung von Redigierbaren Signaturschemata
- Konkrete e-Business Anwendungen

10.50 Uhr **Kommunikationspause**

Rechtliche Aspekte & Ethik • Leitung: F. Freiling — A

11.20 Uhr **Löschpflichten – Wie lange dürfen Daten aufbewahrt werden** — **D. Hausen**, SSW Schneider Schiffer Weihermüller
- Vorgaben von EU (RL 95/46/EG, DS-GVO) und Bundesdatenschutzgesetz
- Anforderungen an ein „datenschutzgerechtes“ Löschen
- Regellöschfristen und Löschkonzepte
- Speicherung von Daten über Altkunden?
- Wann endet die Einwilligung in die Speicherung?

11.45 Uhr **Ethik in der Sicherheitsforschung** — **S. Schrittwieser**, TU Wien, **E. Weippl**, **M. Mulazzani**, **S. Panhans**, SBA Research
- Ethische Fragen in der quantitativen, deskriptiven Sicherheitsforschung
- Grundlegende ethische Prinzipien der Forschung
- Anwendbarkeit des Menlo-Reports
- Vergleich der ethischen Argumentation richtungsweisender Forschungsarbeiten
- Ausblick und weitere Entwicklung

12.10 Uhr **Faktoren des datenschutzbewussten Verhaltens in Facebook** — **N. Hintz**, **Z. Benenson**, Uni Erlangen-Nürnberg
- Umgang mit privaten Daten in Facebook
- Einflussfaktoren auf Benutzerverhalten
- Fake-Accounts bei Facebook
- Der Beziehungsstatus als Einflussfaktor für den Umgang mit eigenen Daten
- Religion als Einflussfaktor für den Umgang mit eigenen Daten

12.35 Uhr **Gemeinsame Mittagspause**

Dienstag • 17. September 2013

IT-Sec-Management • Leitung: W. Schäfer — A

13.35 Uhr **Pflege und Fortschreibung von IT-Grundschutzkonzepten** — **F. Rustemeyer**, HiSolutions AG

- IT-Grundschutz ist als Methodik für Sicherheitskonzepte Standard
- In den letzten Jahren wurden viele solche Konzepte erstellt
- Diese Konzepte stehen nun zur Aktualisierung an
- Wie ist eine Fortschreibung mit begrenztem Aufwand möglich?
- Welche Herausforderungen sind dabei zu beachten?

14.00 Uhr **Security Risk Assessment Framework** — **A. Beck**, **M. Trojahn**, **F. Ortmeier**, Uni Magdeburg

- Automatisierte Sicherheitsbewertungen als Grundlage effizienten Handelns
- Aggregation von Standard-Metriken als vergleichbare Bewertungsmatrix
- Ganzheitliche Betrachtung der Sicherheit einer Systemlandschaft
- Verbesserung der Sicherheitsbewertungen durch maschinelles Lernen
- Ausblick und Weiterentwicklung der Methodik sowie Chancen

14.25 Uhr **BSI-Leitfaden zur Entwicklung sicherer Webanwendungen** — **A. Salkic**, SEC Consult

- Risiken unsicherer Software
- Vermeidung sowie frühzeitige Beseitigung von Sicherheitslücken
- Einführung eines Secure Development Lifecycle in der Organisation
- Vorgaben an den Entwicklungsprozess und an die Implementierung
- Berücksichtigung der Sichtweise von Auftraggeber und Auftragnehmer

14.50 Uhr **Automatisierte Überprüfung der IT-Compliance** — **M. Krambrich**, **R. Grimm**, Uni Koblenz-Landau, **A. Meletiadou**, buw Unternehmensgruppe

- IT-Compliance: Sicherheitsmaßnahmen und deren Überprüfung
- Realisierung eines ISMS auf Basis von IT-Grundschutz
- Definition einer Methodik für die Automatisierbarkeit
- Automatisierte Maßnahmenüberprüfung: Vor- und Nachteile
- Ausführung von Sicherheitstests mit dem Tool OpenVAS

Cloud & Virtualisierung • Leitung: J. Neuschwander — B

13.35 Uhr **Design und Implementierung von Virtual Security Appliances** — **K.-O. Detken**, DECOIT GmbH

- Simulation von Server- und Netzwerkkomponenten
- Virtuelle Umgebungen analysieren und ausrollen
- Erheben einer bestehenden IT-Infrastruktur
- Einsatz von sogenannten Virtual Security Appliances (VSA)
- Automatisierte Konfiguration von VSAs

14.00 Uhr **Mobiler Datenaustausch in der Cloud mit Zertifikaten** — **G. Jacobson**, Secardeo GmbH

- Cloud Security mit PKI
- Public Key Verschlüsselung in Online-Speicherdiensten
- Datenaustausch mit Jedermann mittels Zertifikats-Cloud
- Verschlüsselung mit X.509 Zertifikaten an mobilen Endgeräten
- Anwenderfreundliche Encryption Apps für Android, iOS & Co.

14.25 Uhr **Sicheres Speichern in der Public Cloud mittels Smart Cards** — **B. Zwattendorfer**, EGIZ, **B. Suzic, P. Teufl**, A-SIT, **A. Derler**, TU-Graz

- Sicheres Speichern in der Public Cloud
- Verwendung von Smart Cards (Österreichische Bürgerkarte)
- Aufbauend auf dem Open Source-Tool Citizen Card Encrypted (CCE)
- Unterstützung von Gruppenverschlüsselung und externer PKI
- Plattformunabhängigkeit und Vermeidung von Vendor Lock-In

14.50 Uhr **Topologie-Editoren zur graphischen Konzeption von VSAs** — **K.-O. Detken**, DECOIT GmbH, **E. Eren**, FH Dortmund

- Konzeption und Steuerung von Netztopologien
- Vorstellung unterschiedlicher Editoren: Virtual Wizard, Topologie Editor, etc.
- Vergleich der drei Editoren
- Umsetzung der Compliance in virtueller Umgebung
- Einsatzmöglichkeiten

15.15 Uhr Kommunikationspause

Dienstag • 17. September 2013

Smartphone & Mobile Security • Leitung: W. Kühnhauser — A

15.45 Uhr **Biometrische Alternativen zum Habenfaktor bei Smartphones** — **M. Trojahn**
- Kriterien zum Vergleich von Authentifizierungsverfahren — **A. Beck**
- State-of-the-art BESITZ-Faktoren — Volkswagen AG
- Möglichkeiten durch Sensoren im Smartphone — **F. Ortmeier**
- Biometrische Lösungen für Authentifizierungsmethoden — Uni Magdeburg
- Vergleich der Methoden

16.10 Uhr **Sichere Smartphoneplattform** — **R. Krüger**
- MDM, Container und was noch? — secunet Security
- Von sicherer Telephonie bis zur sicheren Plattform — Networks AG
- Externe und integrierte Sicherheitsanker
- Vergleich der einzelnen Ansätze
- Praxisbeispiele und Ausblick

16.35 Uhr **Vertrauenswürdigkeit für mobile Apps** — **U. Oesing**
- Modultests für mobile Apps auch durch Wissensträger? — Hochschule
- Testen Sie, was funktionieren soll! — Bochum
- Testen Sie, was nicht funktionieren darf! — **R. Krüger**
- Sicherheit für mobile Apps durch Vermeidung undefinierter Zustände — secunet Security
- Praxisbeispiele und Ausblick — Networks AG

17.00 Uhr **Web Service-Security für Android** — **A. Wahl**
- Web Service Clients auf Android-basierten Geräten — Hochschule
- SOAP-basierte Web Services — Furtwangen
- Umsetzung von Sicherheitsaspekten
- Quelloffene, rein Java-basierte Implementierung des WS-Policy Standards
- Alternative für Anwendungsfälle, in denen JSON und TLS nicht ausreichen

17.25 Uhr **Ende erster Konferenztag**

18.30 Uhr **Gemeinsames Abendessen**

Mittwoch • 18. September 2013

IT-Sicherheit im Automotive-Umfeld • Leitung: E. Weippl — A

09.00 Uhr **Automotive IT-Forensik am Beispiel des BSI Leitfadens** — **S. Kuhlmann**
- Reflektion des Leitfadens IT-Forensik für automotive Anwendungen — **J. Dittmann**
- Voraussetzungen: Datenarten, Speicher und Zugriff im Fahrzeug — **T. Hoppe**
- Vorschläge zur Anpassung und Erweiterung für Fahrzeug-IT-Forensik — **S. Kiltz**
- Skizzierung eines praxisrelevanten Beispiels — **W. Menzel**
- Anwendungsgebiete und Nutzen für verschiedene Zielgruppen — OvGU / FIN / ITI

09.25 Uhr **Biometrische Authentifizierung zur Fahrererkennung in LKWs** — **M. Trojahn**
- Vergleich von Lösungen zur Fahrererkennung — **A. Beck**
- Aktuelle Methoden für Lenkzeitkontrollen — Volkswagen AG
- Grundlagen für biometrische Zugriffssysteme — **F. Ortmeier**
- Biometrische Authentifizierungsmethoden im Lkw-Cockpit — Uni Magdeburg
- Herausforderungen bei der biometrischen Authentifizierung

09.50 Uhr **Simulation von Vorfallsfolgen in Car-to-X Testumgebungen** — **T. Hoppe**
- Car-to-X: Kurzeinführung und Stand der Technik/Forschung — **S. Kuhlmann**
- Vorstellung verfügbarer Entwicklungs-/Testumgebungen für C2X — **S. Kiltz**
- Nutzung zur Simulation exemplarischer Angriffsszenarien — **J. Dittmann**
- Abschätzung der Folgen und Reflektion für zukünftige Produktivsysteme — Uni Magdeburg
- Diskussion von Maßnahmen der Prävention, Detektion und Reaktion

10.15 Uhr Kommunikationspause

Webanwendungen & Sicherheitsinfrastrukturen • Leitung: M. Hartmann — A

10.45 Uhr **Effizientes Testen von E-Government-Komponenten in der Cloud** — **V. Krnjic**
- Anforderungen von E-Government-Komponenten an Testframeworks — **P. Weber**
- Analyse von bestehenden Testframeworks — **T. Zefferer**
- Evaluierung des entwickelten Cloud-basierten Frameworks — **B. Zwattendorfer**
- Plattformübergreifende Tests von E-Government-Komponenten — TU Graz
- Evaluierung des Frameworks

11.10 Uhr **Schutz von Datenbanken vor fehlerhaften Webanwendungen** — **P. Trommler**
- Schutz gegen Insecure Direct Object References — **B. Große**
- Defence in Depth durch feingranulare Zugriffskontrolle — **S. Prijovic**
- Security Appliance mit zwei Proxies — Ohm-Hochschule
- Zuordnung Webanfragen zu Datenbankabfragen — Nürnberg
- Konfiguration des Zuordnungsmechanismus

11.35 Uhr **Sicherer Schlüssel- und Informationsaustausch mit SAML** — **D. Felsch**
- Authentischer Transport von beliebigem Schlüsselmaterial mittels XML — **F. Feldmann**
- Sec²: Vertrauliches kollaboratives Arbeiten in der Cloud — **C. Meyer**
- SAML: Mehr als nur Single-Sign-On — **T. Schreiber**
- Bindung von kryptographischen Schlüsseln an Identitäten — **J. Schwenk**
- Standardkonform: Bestehende Implementierungen weiter nutzbar — Uni Bochum

12.00 Uhr **Leichtgewichtige Sicherheitsdomänen für spontane Kooperationen** — **W. Kühnhauser**
- Sensitive Daten auf mobilen Systemen — **P. Amthor**
- Smartphone-Sicherheit — TU Ilmenau
- Spontane Kooperationen mobiler Systeme
- Algebraisch gesteuerte Erzeugung von Sicherheitspolitiken
- Implementierung von Sicherheitspolitiken auf Android/MOSES Plattformen

Workshop der GI-FG SECMGT • Leitung: I. Münch und B. Witt — B

10.45 Uhr **ISIS12 – Informationssicherheit für mittelständische Unternehmen** — **M. Gruber**, BSP. SECURITY
- ISMS light für den Mittelstand
- Integration von ISMS und IT-SM
- Pragmatisches 12-stufiges Verfahrensmodell
- Vorstufe zu BSI IT Grundschutz bzw. ISO/IEC 27001
- Möglichkeit zu einer ISIS12-Zertifizierung

11.35 Uhr **Der externe (IT-)Sicherheitsbeauftragte** — **C. Friedrich**, HiSolutions AG
- Ein externer SiBe (ESB) ist nur mit Unterstützung der Leitung erfolgreich
- Qualifizierte ESB können einen internen Sicherheitsbeauftragten ersetzen
- Potentielle Risiken beim Einsatz eines ESB müssen beachtet werden
- Kosten für ESB können einen schnelleren Aufbau des ISMS ermöglichen
- ESB sollten beim Aufbau des internen ISMS-Know-Hows unterstützen

12.25 Uhr **Gemeinsame Mittagspause**

Netzwerksimulation & Netzwerksicherheit • Leitung: P. Trommler — A

13.25 Uhr **Sicherheit auf Basis Multikriterieller Spieltheorie** — **S. Rass**, Uni Klagenfurt
- Quantitatives Risiko-Management
- Multikriterien-Entscheidungen — **S. Schauer**, AIT
- Forschungsprojekt: „Risikomanagement für simultane Bedrohungen“
- Szenario-Analysen und das Doppelvektor-Modell — **A. Peer, J. Göllner**, BMLVS
- Sicherheitsanalysen durch Spieltheorie

13.50 Uhr **Wer spielt, gewinnt** — **M. Schrattenholzer**, **M. Ruzicka**, **M. Rybnicek**, **R. Poisel**, **S. Tjoa**, FH St. Pölten
- Simulation von kritischen Infrastrukturen
- Agenten-basierte Modellierung von Risikoindikatoren
- Spieltheoretische Umsetzung von Agentenverhalten
- Regelbasiertes Programmieren mit Excel
- Privacy Aspekte in verteilten Simulationen

14.15 Uhr **CADEMI – Cooperative Anomaly Detection and Mitigation** — **J. Steinberger**, **S. Abt**, **H. Baier**, Hochschule Darmstadt
- Netzwerksicherheit auf der Ebene von Hochverkehrsknoten
- Flow-basierte Analyse von Netzwerkdaten
- Detektion, Mitigation und Reaktion
- Klassifikation von Netzwerkanomalien
- Ereignisverarbeitung

14.40 Uhr **Kommunikationspause**

Mittwoch • 18. September 2013

Zukünftige Infrastrukturen & Produkte • Leitung: A. Philipp — A

15.10 Uhr **Die Gefahr fehlender Passwörter in Heimfernsteuerungen** — **R. Reitze**, **P. Helmig**, INSIDERS-KNOWLEDGE

- Netzwerkgeräte werden mit unsicherer Standardkonfiguration ausgeliefert
- Shodan-Suchmaschine erlaubt die Suche nach unsicheren Geräten
- Hersteller müssen Sicherheitsrisiken durch Benutzerfehler minimieren
- Herausforderung: User-friendly vs. User-proof
- Fallbeispiele Netzwerkspeicher und Heimfernsteuerung

15.35 Uhr **Datenübertragung in Smart Grids mit Trusted Computing** — **R. Sethmann**, **O. Hoffmann**, **S. Busch**, Hochschule Bremen

- Sicherheitskonzept für Smart Grids
- Technische Richtlinie BSI TR-03109 SMART ENERGY berücksichtigt
- Einsatz von Trusted Network Connect (TNC) in Smart Grids
- Absicherung des Smart Meter Gateways durch den TPM-Chip
- Umsetzung des Sicherheitskonzeptes im Demonstrator validiert

16.00 Uhr **Manipulationssensible Kopierschutzfolien** — **M. Hennig**, **O. Schimmel**, **P. Zieris**, **G. Sigl**, Fraunhofer AISEC

- Sensorik zur Manipulationsdetektion in eingebetteten Systemen
- Maßnahmen gegen „Reverse Engineering" durch eine Schutzfolie
- Schlüsselgenerierung mittels physikalischer Folieneigenschaften
- Untrennbare Koppelung von Hard- und Software gegen Produktpiraterie
- Sicherer Hardwareanker in einer sicherheitskritischen Umgebung

16.25 Uhr **Konferenzende**

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

Aufbau eines kennzahlenbasierten Übungsprogrammes — **R. Kroha**, **M. Köppe**, **I. Reiffersberger**, HiSolutions AG

- Risikobasierte Übungsplanung
- Kontinuierliche Verbesserung durch Einsatz von Kennzahlen
- Nachhaltige Steigerung der Resilienz durch mittelfristige Planung
- Erhöhung der Wirtschaftlichkeit durch Einsatz geeigneter Technik
- Praxisbeispiel: Das Rahmenwerk für IT-Notfall und -Krisenübungen des BSI

Ein Vorgehensmodell für die digitalisierte Schlossforensik — **S. Kiltz**, **E. Clausing**, **J. Dittmann**, **C. Vielhauer**, Uni Magdeburg

- Kontaktlose Oberflächenmesstechnik für die Schlossuntersuchung
- Vollständig digitale Untersuchung mittels Mustererkennung
- Konsolidierung der Sichten von forensischen Experten und Informatikern
- Vorgehensmodell für digitalisierte Forensik – Kritik und Erweiterung
- Abbildung von Detailsichten der Untersuchung auf das Vorgehensmodell

Die Beiträge dieser Referenten finden Sie auch im Tagungsband zur Konferenz

Anmeldung & Teilnahmebedingungen

D·A·CH Security 2013

17. und 18. September 2013
Georg-Simon-Ohm-Hochschule Nürnberg

Anmeldung zur Konferenz

Telefon: +43 (0) 463 2700 3702
Fax: +43 (0) 463 2700 993702 oder
Online-Anmeldung unter: http://www.syssec.at/ds13_anmeldung

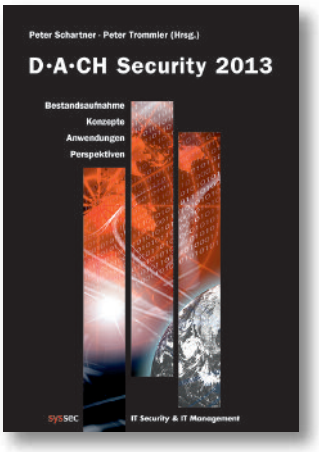
Teilnahmebedingungen

Bei Anmeldung bis zum bis 16. August 2013 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 9. August 2013 (Datum des Poststempels) wird eine Bearbeitungsgebühr von € 75.– erhoben. Nach dem 9. August 2013 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

Leitungsgremium der Konferenzreihe

P. Horster Uni Klagenfurt • **P. Schartner** Uni Klagenfurt

Programmkomitee

Vorsitz: **P. Schartner** Uni Klagenfurt • **P. Trommler** Georg-Simon-Ohm-Hochschule Nürnberg

R. Ackermann SAP Research • **P. Beenken** Porsche AG • **J. Dittmann** Uni Magdeburg • **D. Engel** FH Salzburg, **F. Freiling** Uni Erlangen-Nürnberg • **J. Fuß** FH Hagenberg • **M. Hartmann** SAP • **P. Horster** Uni Klagenfurt **D. Hühnlein** ecsec GmbH • **S. Janisch** Uni Salzburg • **K. Knorr** HS Trier • **T. Kob** HiSolutions AG **U. Korte** BSI • **P. Kraaibeek** secunet • **W. Kühnhauser** Uni Ilmenau • **P.J. Kunz** Daimler • **S. Lechner** JRC **H. Leitold** A-SIT • **H. Mühlbauer** TeleTrusT • **I. Münch** BSI • **J. Neuschwander** HTWG Konstanz **A. Philipp** Utimaco • **N. Pohlmann** FH Gelsenkirchen • **R. Posch** TU Graz • **W. Rankl** Giesecke & Devrient **S. Rass** Universität Klagenfurt • **H. Reimer** DuD • **A. Roßnagel** Uni GH Kassel • **W. Schäfer** DATEV **H. Storck** Nokia Siemens • **S. Teufel** Uni Fribourg • **G. Weck** Infodas • **C. Wegener** Uni Bochum **E. Weippl** SBA Research • **G. Welsch** 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 & Co. KG

K. Kirst PTLV • **J. Nedon** IABG mbH • **P. Reymann** ITQS • **C. Stark** Citigroup AG • **D. Schadt** SPOT Consulting

Organisation

D. Cechak Uni Klagenfurt • **P. Schartner** Uni Klagenfurt
P. Trommler Georg-Simon-Ohm-Hochschule Nürnberg • **M. Möhlmann**