Seminarort

CCG-Zentrum, Technologiepark Argelsrieder Feld 11
D-82234 Weßling-Oberpfaffenhofen

Eine Lageskizze sowie Hinweise für die Anreise und Übernachtung schicken wir Ihnen mit der Bestätigung der Anmeldung zu.

Gebühr

EUR 1.495,--
Die CCG ist ein gemeinnütziger Verein und in Deutschland von der Umsatzsteuer befreit. Für Veranstaltungen an ausländischen Standorten gelten die dortigen Steuerregelungen.

Mitglieder der CCG erhalten 10% Rabatt. Bei Anmeldung mehrerer Mitarbeiter einer Firma / Dienststelle zum gleichen Seminar erhält jeder Teilnehmer 10%. Studentenrabatte sind auf Nachfrage verfügbar. Die Rabatte sind nicht miteinander kombinierbar.

Bitte zahlen Sie bargeldlos nach Erhalt der Rechnung.

Anmeldungen

Bitte möglichst bis 3 Wochen vor Seminarbeginn an:

Carl-Cranz-Gesellschaft e.V., Argelsrieder Feld 11, D-82234 Weßling
Tel. +49 (0) 8153 / 88 11 98 -12, Fax -19, E-Mail: anmelden@ccg-ev.de
Internet: www.ccg-ev.de

Die Anmeldungen werden schriftlich bestätigt.

Weitere Informationen zum Inhalt

K.-D. Wolfenstetter, ehem. Deutsche Telekom AG, Laboratories, Berlin
E-Mail: k.wolfenstetter@t-online.de

Stornierung

Bei Stornierung mündlich oder schriftlich bestätigter Anmeldungen wird eine Bearbeitungsgebühr von EUR 25,-- berechnet. Bei Stornierungen, die später als 10 Tage vor Seminarbeginn eingehen, werden 25% der Gebühr, bei Nichterscheinen die volle Gebühr in Rechnung gestellt. Die Vertretung eines angemeldeten Teilnehmers ist möglich.

Ausfall von Seminaren oder Dozenten

Die CCG behält sich vor, bei zu geringer Teilnehmerzahl oder aus anderen triftigen Gründen ein Seminar bis 10 Tage vor Beginn abzusagen. Sie behält sich weiter vor, entgegen der Ankündigung im Programm auch kurzfristig einen Dozenten und evtl. auch dessen Thema zu ersetzen. Ein Schadensersatzanspruch bleibt ausgeschlossen.

Ganzheitliche Sicherheit

Teilnehmer

- Datenschutz- und Datensicherheitsbeauftragte und -verantwortliche
- CSOs und CISOs in Unternehmen und Behörden
- Compliance-Verantwortliche
- Studierende und Mitarbeiter in den MINT-Fächern

Seminarinhalte

Einerseits bietet die mathematisch begründete Kryptographie ein festes Fundament für jede Sicherheitslösung. Andererseits bietet deren Implementierung und Realisierung etwa in SW, aber auch in HW, mögliche Angriffsflächen für technologisch gut ausgerüstete Angreifer. Ein guter kryptographischer Algorithmus ist dann wertlos, wenn z. B. seine geheimen Schlüssel im realisierenden Medium (Chip, Rechner, Handy) ausgespäht werden können.

Das Seminar umfasst in einer ganzheitlichen Sicht den kompletten Zyklus von den kryptographischen Methoden (z. B. RSA, AES) über deren Anwendungen und Einsatzszenarien (Internet, Mobilkommunikation) bis hin zu modernsten Angriffsmethoden aus der Praxis (Optische Emission, Reverse Engineering, HW Trojaner).

Vortragende

A. Beutelspacher	Prof. Dr.	Universität Gießen Mathematisches Institut
J.-P. Seifert	Prof. Dr.	TU Berlin
K.-D. Wolfenstetter	Dipl.-Math.	ehem. Deutsche Telekom AG, Laboratories, Berlin KDWsec

Unterlagen

Jeder Teilnehmer erhält die Vortragsunterlagen.
Die Kosten dafür sind in der Gebühr enthalten.

Carl-Cranz-Gesellschaft e.V. | Weßling

Gesellschaft für technisch-wissenschaftliche Weiterbildung

Seminar IN 6.27

Ganzheitliche Sicherheit: Von der Kryptographie bis zu Physical Unclonable Functions

21. – 23. September 2021
Oberpfaffenhofen bei München

Informatik

Wissenschaftliche Leitung

Dipl.-Math. K.-D. Wolfenstetter
ehem. Deutsche Telekom AG, Laboratories, Berlin; KDWsec

Seminarprogramm

Dienstag, 21.9.2021
10.15 – 16.30 Uhr

10.15 – 10.30	Begrüßung, Einführung, Organisation
10.30 – 12.00 A. Beutelspacher	**Ziele und Probleme der Kryptographie**
13.00 – 14.30 A. Beutelspacher	**Symmetrische Verschlüsselungsverfahren** Data Encryption Standard DES
	Modes of Operation
	Advanced Encryption Standard AES
	Kryptoanalyse
15.00 – 16.30 A. Beutelspacher	**Public Key Kryptographie** RSA und Diffie Hellman
	Digitale Signaturen, Zertifikate, PKI
	Verfahren auf Basis des Diskreten Logarithmus
	Elliptische Kurven Kryptographie

Mittwoch, 22.9.2021
08.30 – 16.30 Uhr

08.30 – 10.00 J.-P. Seifert	**Probleme und Herausforderungen technologischer Sicherheit** Implementierungen und Realisierungen
	Das Ende von Moore's Law und Non-volatile Memo
10.30 – 12.00 J.-P. Seifert	**Neue Angriffsmethoden aus der Praxis** Focus Ion Beam, Optische Emission und Fehler Induktionsmethoden
	Hardware Trojaner
	Reverse Engineering von Chips
13.00 – 14.30 J.-P. Seifert	**Neue Entwicklungen in der Sicherheitstechnologie** Physical Unclonable Functions (PUFs)
	Obfuscation oder leakage-resilient Kryptographie zur Umgehung der Grenzen
15.00 – 16.30 J.-P. Seifert	**Grenzen der heutigen Implementierungen bzgl. Sicherheit**

Donnerstag, 23.9.2021
08.30 – 16.30 Uhr

08.30 – 10.00 K.-D. Wolfenstetter	**Anwendungsfelder von Kryptographie und Sicherheitstechnologie** Sicherheitsstandards in der Mobilkommunikation; Angriffsarten und Risikobetrachtungen
	Sicherheit im Internet: Layer-Sicherheit und ihre Grenzen; IPv6; Browser; eMail
10.30 – 12.00 K.-D. Wolfenstetter	**Spezielle Szenarien der Sicherheit** Smart Meter und Smart Meter Gateway in Energienetzen
	eCards: Neuer Personalausweis, Gesundheitskarten, Payment und mWallet
13.00 – 14.30 K.-D. Wolfenstetter	**Neue Entwicklungen und Herausforderungen für die Sicherheit** Embedded Security; Industrie 4.0
	Blockchain und Kryptographie
	Quantum Computing und Kryptographie
15.00 – 16.30 K.-D. Wolfenstetter	**Ganzheitliche Sicherheit** Technologische und regulatorische Grenzen der Sicherheit
	Pro und contra Kryptoregulierung
	Die neue EU-Verordnung EIDAS: Sicherheit für den Binnenmarkt
	IT-Sicherheitsgesetz(e)

Weitere Seminare zum Themenbereich

- „Einführung in das Quantum Computing und seine Anwendungen", 18.–20.5.2021 (Code IN 5.20)
- „Kryptografie - eine Schlüsseltechnik zur Gestaltung zukünftiger Informationstechnik", 7.–8.6.2021 (Code IN 6.17)
- „Datenschutz für Softwareentwicklung und IT-Beratung", 1.7.2021 (Code IN 6.45)
- „Post-Quantum Sichere Verschlüsselungsverfahren", 29.–30.9.2021 (Code IN 6.46)