

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 999,-

Die CCG ist als gemeinnützig anerkannt und von der USt befreit.

Mitglieder der CCG erhalten 10% Rabatt, Studenten bei Vorlage des
Studentenausweises 75%. Bei Anmeldung mehrerer Mitarbeiter einer
Firma / Dienststelle zum gleichen Seminar erhält jeder Teilnehmer 10%.

Die Rabatte sind nicht miteinander kombinierbar.

Bitte zahlen Sie bargeldlos nach Erhalt der Rechnung.

Anmeldungen

Bitte möglichst bis 14 Tage vor Seminarbeginn an:

Carl-Cranz-Gesellschaft e.V., Postfach 11 12, D-82230 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

Prof. Dr. Rainer Böhme
Westfälische Wilhelms-Universität Münster
Institut für Wirtschaftsinformatik, Juniorprofessur für IT-Sicherheit
Leonardo-Campus 3, D-48149 Münster
Tel. +49 (0) 251 / 83-38250
E-Mail: rainer.boehme@wi.uni-muenster.de

Stornierung

Bei Stornierung mündlich oder schriftlich bestätigter Anmeldungen wird
eine Bearbeitungsgebühr von EUR 25,- berechnet. Bei Stornierungen,
die später als 7 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.

Teilnehmer

Das Seminar vermittelt vertiefte Kenntnisse über Konzepte und Techniken
der digitalen Multimediaforensik. Angesprochen sind insbesondere
Interessenten aus den Bereichen Sicherheit, Strafverfolgung, Industrie
und Medien. Die Teilnehmer erhalten einen Überblick zu relevanten
Analysemethoden und lernen dabei, die Authentizität digitaler Mediendaten
mittels forensischer Methoden kritisch zu überprüfen. Einen Schwerpunkt
bildet die Analyse digitaler Bilder. Neben der Vermittlung der
entsprechenden Theorie zeichnet sich das Seminar dank zahlreicher
Demonstration durch einen starken Bezug zur Praxis aus.

Seminarinhalte

Digitale Multimediaforensik ist ein Sammelbegriff für forensische Techniken,
die eine systematische Überprüfung der Authentizität digitaler
Mediendaten zum Ziel haben.

Die weite Verbreitung von digitaler Aufnahmetechnik gepaart mit immer
besserer Bearbeitungssoftware erlaubt es selbst unbedarften Nutzern,
digitale oder digitalisierte Mediendaten täuschend echt zu manipulieren.
Die Authentizität von Mediendaten ist aber überaus bedeutsam, wenn
diese zur Entscheidungsfindung herangezogen werden, wie etwa vor
Gericht (Beweisfotos), in den Naturwissenschaften (Ergebnisdokumentation)
aber auch bei der Bildung von öffentlicher Meinung (Pressefotos).

In letzter Zeit gewinnt daher verstärkt das Feld der digitalen Multimediaforensik
an wissenschaftlichem Interesse und ist aktuell eines der spannendsten
und meist diskutierten Forschungsfelder im Bereich der Multimedia-
sicherheit. Anders als bisherige Ansätze zur Überprüfung der
Authentizität digitaler Mediendaten (etwa auf Basis kryptographischer
Verfahren oder digitaler Wasserzeichen) benötigen Verfahren der
Multimediaforensik keinerlei Wissen über ein etwaiges Original. Allein
durch eine statistische Analyse der Mediendaten ergeben sich praktisch
unbegrenzte Anwendungsszenarien bei der Aufdeckung von Manipulationen
und der Bestimmung der Herkunft von digitalen Mediendaten.

Vortragende

R. Böhme	Prof. Dr.	WWU Münster
M. Kirchner	Dipl.-Ing.	
T. Gloe	Dipl.-Medieninf.	TU Dresden

Unterlagen

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

Seminar IN 9.20

Digitale Multimediaforensik

29. – 30. November 2011
Oberpfaffenhofen bei München

Wissenschaftliche Leitung

Prof. Dr. Rainer Böhme
WWU Münster

Seminarprogramm

Dienstag, 29.11.2011

09.00 – 16.30 Uhr

- 09.00 – 09.15 Begrüßung, Organisation
- 09.15 – 10.30 **Einführung**
R. Böhme
Ziele forensischer Techniken • Einordnung • Abgrenzung von aktiver Authentikation, Computerforensik und computerunterstützter Forensik • digitale Bilder und deren Entstehung • Grundlagen der Multimediaforensik: Gerätecharakteristiken und Manipulationsartefakte • „Legitimität“ von Bildbearbeitung • Beispiele
- 11.00 – 12.00 **Herkunftsbestimmung und Integritätsprüfung digitaler Bilder anhand von Meta-Daten**
T. Gloe
Überblick zu gängigen Dateiformaten • Was sind Meta-Daten und wie können sie für forensische Zwecke genutzt werden? • Bildrepräsentation im Orts- und Frequenzraum • Exiftool • JPEG Snoop • Vorschaubilder • Analyse der JPEG-Quantisierungstabelle • Demonstration
- 13.00 – 14.30 **Herkunftsbestimmung digitaler Bilder anhand von Signaleigenschaften I**
T. Gloe
Techniken zur Bestimmung der Geräteklasse und des Gerätetyps • Erkennung computergenerierter Bilder • Unterscheidung von Scannern und Digitalkameras • Zeilen- und Spaltensensoren • Unterscheidung von Kameramodellen • Schätzung der JPEG-Quantisierungstabelle • merkmalsbasierte Verfahren • Rauschcharakteristiken • Farbwiedergabe • Abbildungsfehler • Leistungsfähigkeit der Verfahren • Robustheit
- 15.00 – 16.30 **Herkunftsbestimmung digitaler Bilder anhand von Signaleigenschaften II**
T. Gloe
Techniken zur Bestimmung einzelner Geräte • Analyse defekter Sensorelemente und Schmutzmuster • Sensorrauschmuster • Schätzung des Rauschmusters • Korrelationsdetektor • Berücksichtigung von Ausreißern • optimaler Detektor • Resynchronisation nach geometrischen Transformationen • Image-Digest • Demonstration
- ab ca. 17.30 **Social Event**
Führung durch die Münchener Altstadt (optional)

Mittwoch, 30.11.2011

08.30 – 15.45 Uhr

- 08.30 – 10.00 **Prüfung der Integrität digitaler Bilder anhand von Signaleigenschaften des Geräts**
M. Kirchner
Color Filter Array • Farbinterpolation • Layout • Erkennung und Identifikation • Integrität der Sensorrauschmuster • Erkennung von Beschneidung • Artefakte der JPEG-Kompression • Schätzung der Blockgrenzen • Ausrichtung der Blockgrenzen • Doppelkompression • Nutzbarkeit von Abbildungsfehlern • chromatische Abberation • Verzeichnung • Demonstration
- 10.30 – 12.00 **Prüfung der Integrität digitaler Bilder anhand von Manipulationsartefakten**
M. Kirchner
Copy-Move-Erkennung • Merkmalsrepräsentation • Ordnung und effiziente Suche • Nutzbarkeit von Splicing-Features zur Erkennung von Montagen • Erkennung von Resampling • periodische Artefakte • Spektralanalyse der „P-Map“ • Interpretation von Peaks • Wirkung von linearen und nicht-linearen Filtern • Demonstration
- 13.00 – 14.30 **Überblick über weitere Techniken**
R. Böhme
Audioforensik durch Netzfrequenzanalyse • Übertragbarkeit der Verfahren auf Videoforensik • Bildanalyse auf semantischer Ebene • Analyse der Beleuchtungssituation • Grenzen forensischer Analysen • Techniken zur Vereitelung des Erfolgs forensischer Analysen • Steganalyse • Bildforensik in der Praxis
- 15.00 – 15.45 **Zusammenfassung und Diskussion**
alle Referenten
Gelegenheit für spezielle Fragen der Teilnehmer

Unterlagen

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

Weitere Seminare zum Themenbereich

- „Bildverarbeitung und Bewegtbildanalyse“, 27.–29.2.2012 (Code IN 9.02)
- „Kryptographie – eine Schlüsseltechnik zur Gestaltung zukünftiger Informationstechnik“, 28.–29.3.2012
- „Digitale Signalanalyse – moderne Verfahren und Anwendungen“, 16.–18.10.2012 (Code FA 9.18)