Horst Görtz Institut
für Sicherheit in der Informationstechnik

HGI-News

Horst Görtz Institut für Sicherheit in der Informationstechnik
Ruhr-Universität Bochum, Universitätsstr. 150, D-44780 Bochum
Tel.: +49 - (0)234 - 32 23262, Fax.: +49 – (0)234 – 32 14430
Web: http://www.hgi.ruhr-uni-bochum.de

Nr. 04 Montag, 1. September 2003

VERANSTALTUNGEN DIESES MONATS / ACTIVITIES OF THIS MONTH

Mittwoch / Wednesday
Workshop on Crytographic Hardware and Embedded Systems 2003 (CHES 2003)

10.09.2003
08.45 Uhr, Hilton Hotel, Köln
Prof. Dr. Hans Dobbertin, Lehrstuhl für Informationssicherheit und Kryptologie, RUB
„Algebraic Structures in AES – Cryptographically Strong or Risky?“

Mittwoch / Wednesday
Workshop on Crytographic Hardware and Embedded Systems 2003 (CHES 2003)

10.09.2003
11.30 Uhr, Hilton Hotel, Köln
Jan Pelzl, Lehrstuhl für Kommunikationssicherheit
„Hyperellictic Curve Cryptosystems: Closing the Performance Gap to Elliptic Curves“

ANKÜNDIGUNG / ANNOUNCEMENT

HGI KOLLOQUIUM „E-CRM IM PUBLIC SECTOR“

15.10.2003, 14.00 Uhr
NA 1/51 (Friedrich Sommer Raum), Ruhr-Universität Bochum

Sebastian Tengler, Lehrstuhl für Produktionswirtschaft, Ruhr-Universität Bochum
„Die Bedeutung der Informationssicherheit am Beispiel von CRM und SCM"

Utz Helmuth, Geschäftsführer cosinex GmbH, Witten
Der Titel wird noch bekannt gegeben.

VERÖFFENTLICHUNGEN / PUBLICATIONS

Prof. Dr. Marion Steven, Sebastian Tengler, Rolf Krüger . "Reverse Logistic (I)". Das Wirtschaftsstudium. 2003, Heft 5, S. 643-647.

Prof. Dr. Marion Steven, Sebastian Tengler, Rolf Krüger . "Reverse Logistic (II)". Das Wirtschaftsstudium. 2003, Heft 6, S. 779-784.

KONGRESSE, TAGUNGEN, FORSCHUNGSAUFENTHALTE / CONGRESSES, MEETINGS, RESEARCH ABROAD

Prof. Dr.-Ing. Paar bot vom 17.-19.08.2003 auf der Hot Chips Conference an der Stanford University in Palo Alto, Kalifornien ein halbtägiges Tutorial zu dem Thema „Past and Future of Cryptographic Engineering" an.

Sebastian Tengler war am 26.08.2003 in Köln und hielt dort im Rahmen der Weiterbildung "Fachkauffrau/-mann Einkauf und Logistik" des Bundesverbandes Materialwirtschaft, Einkauf und Logistik e.V. in Köln den Vortrag „Einkaufspolitik und Grundlagen der Logistik".

Thomas Wollinger besucht vom 01.-03.09.2003 die „International Conference on Field Programmable Logic and Applications – FPL 2003" in Lissabon, Portugal. Er hält dort den Vortrag "How Secure are FPGAs in Cryptographic Applications?"

Prof. Dr. Dobbertin, Prof. Dr.-Ing. Paar, Patrick Felke, Marcus Heitmann, Tanja Lange, Gregor Leander, Sandeep Kumar, Jan Pelzl, Kai Schramm, André Weimerskirch und **Thomas Wollinger** besuchen vom 07.-10.09.2003 den Workshop on Cryptographic Hardware and Embedded Systems 2003 (CHES 2003) in Köln. **Prof. Dr. Dobbertin** hält dort einen Invited Talk mit dem Titel "Algebraic Structures in AES – Cryptographically Strong or Risky?". **Jan Pelzl** wird den Vortrag "Hyperelliptic Curve Cryptosystems: Closing the Performance Gap to Elliptic Curves" halten.

Prof. Dr. Dobbertin, Magnus Daum, Patrick Felke, Tanja Lange und **Gregor Leander** sind vom 26.09.-02.10.2003 im Lorentz-Center der Leiden University, Niederlande. **Prof. Dr. Dobbertin** hält dort auf dem Workshop „Mathematics of Cryptology" einen Invited Talk mit dem Titel „Some Mathematics Behind the Design of Block Ciphers".

Prof. Dr.-Ing. Paar hält am 30.09.2003 im Rahmen der Veranstaltung "IT-Security – Branchenfokus Automotive" ein Frühaufsteher-Tutorium mit dem Titel "Eine kurze Einführung in die IT-Sicherheit".

ANKÜNDIGUNGEN DER HGI-PARTNER / ANNOUNCEMENTS BY CO-OPERATING ORGANISATIONS

IT-SECURITY - BRANCHENFOKUS AUTOMOTIVE

30.09.2003
Zentrum für IT-Sicherheit, Lise-Meitner-Allee 4, 44801 Bochum
Veranstalter: IHK im mittleren Ruhrgebiet zu Bochum, SIHK zu Hagen, GITS AG

Jahr für Jahr verursachen Hacker Schäden in Millionenhöhe. Verbotene Datenbankzugriffe, der Diebstahl vertraulicher Kundendaten, Viren im E-Mail-System sind für die Unternehmen zu einer realen Gefahr geworden. Angriffe auf die IT-Systeme können betriebswirtschaftliche Flurschäden anrichten und das Image eines Unternehmens empfindlich treffen.

Dies hat vor allem die Automobilbranche frühzeitig erkannt. Hersteller und Zulieferer haben sich in den letzten Jahren intensiv mit der Informationssicherheit auseinandergesetzt und ihre Systeme zur Abwehr von Hackern und Spionen weiterentwickelt.

Die Veranstalter laden Sie ein, von den Erfahrungen der Automobilbranche zu profitieren. Erfahren Sie, wie das Thema Datensicherheit hier behandelt wird. Lernen Sie die notwendigen Abwehrmaßnahmen kennen, mit denen Sie auch Ihr Unternehmen wirksam schützen können.

Weitere Information und Anmeldung unter: **http://www.bochum.ihk.de** oder **http://www.gits-ag.de**

CALL FOR PAPERS:
DETECTION OF INTRUSIONS AND MALWARE & VULNERABILITY ASSESSMENT (DIMVA 2004)

06./07.07.2004
Dortmund
Veranstalter: Fachgruppe SIDAR der Gesellschaft für Informatik e.V. (GI)

Die Fachgruppe SIDAR (Security - Intrusion Detection and Response) der Gesellschaft für Informatik e.V. beschäftigt sich mit der Erkennung und Beherrschung von Vorfällen der Informationssicherheit und veranstaltet vom 6.-7. Juli 2004 einen Workshop zum Thema Erkennung von Schutzzielverletzungen (Intrusion Detection), Malware-Bekämpfung (Malicious Agents) sowie Ermittlung von Verwundbarkeiten (Vulnerability Assessment).

Ziel des Workshops ist es, eine Übersicht zum Stand der Technik und Praxis in Industrie, Dienstleistung, Verwaltung und Wissenschaft im deutschsprachigen Raum zu geben. Insbesondere sollen Ergebnisse aus den Bereichen Forschung, Entwicklung und Integration vorgestellt, relevante Anwendungen aufgezeigt sowie neue Technologien und daraus resultierende Produktentwicklungen konzeptionell dargestellt werden. Rechtliche Rahmenbedingungen und wirtschaftliche Faktoren sollen ebenfalls betrachtet werden.

Das Programmkomitee lädt ein zur Einreichung von

- vollen Beiträgen über bisherige Ansätze und Erfahrungen sowie laufende Entwicklungen, insbesondere zu Theorie, Entwurf, Implementierung, Analyse und Evaluierung sowie über rechtliche Rahmenbedingungen.

- vollen Beiträgen und Kurzbeiträgen über Praxisstudien und wirtschaftliche Faktoren bei der Einführung oder Anwendung in Referenzprojekten (Fallstudien).

Weitere Informationen unter: **http://www.gi-fg-sidar.de/dimva2004**

Redaktionsschluß für
„HGI – News" Nr. 05
Freitag, 26. September 2003
12.00 Uhr.

Redaktion:
Oliver Rausch
Email: oliver.rausch@ruhr-uni-bochum.de

Aleksandra Sowa (Geschäftsführerin, HGI)
Email: aleksandra.sowa@ruhr-uni-bochum.de

HGI – News by email
Abonnement unter: http://lists.ruhr-uni-bochum.de/mailman/listinfo/hgi-news

Das Archiv vorheriger Ausgaben ist unter http://www.hgi.ruhr-uni-bochum.de erreichbar.