Organisation

Tagungsbüro

Claudia Graute *(Tagungsbüro)*
Universität Dortmund, Fachbereich Informatik,
LS6 - Informationssysteme und Sicherheit,
D-44221 Dortmund
Tel.: +49-231-755-2641, Fax.: +49-231-755-2405
► *dimva2004@gi-fg-sidar.de*

Elke Herrmann *(Vertretung Tagungsbüro)*
Tel.: +49-231-755-2779, Fax.: +49-231-755-2405

Tagungsleitung

Ulrich Flegel *(Vorsitzender der Tagung)*
Universität Dortmund, Fachbereich Informatik,
LS6 - Informationssysteme und Sicherheit,
D-44221 Dortmund
Tel.: +49-231-755-4775, Fax.: +49-231-755-2405
► *ulrich.flegel@udo.edu*

Michael Meier *(Vorsitzender des Programmkomitees)*
Brandenburgische Technische Universität Cottbus,
Institut für Informatik, Lehrstuhl Rechnernetze,
Postfach 10 13 44, D-03013 Cottbus
Tel.: +49-355-69-2028, Fax.: +49-355-69-2127
► *mm@informatik.tu-cottbus.de*

Veranstalter

Fachgruppe SIDAR der Gesellschaft für Informatik e.V.
Wissenschaftszentrum, Ahrstraße 45, 53175 Bonn
Tel.: +49-228-302-145, Fax: +49-228-302-167
► *http://www.gi-ev.de*

In Zusammenarbeit mit:
German Chapter of the ACM
IEEE Task Force on Information Assurance
Universität Dortmund

Organisation

Programmkomitee

Mitglieder:
Thomas Biege *(SuSE Linux AG)*
Roland Büschkes *(T-Mobile)*
Toralv Dirro *(Network Associates)*
Anja Feldmann *(TU München)*
Ulrich Flegel (stv. Vorsitz) *(Uni Dortmund)*
Christian Freckmann *(TÜV-IT)*
Oliver Göbel *(RUS-CERT)*
Christian Götz *(Cirosec)*
Dirk Häger *(BSI)*
Marc Heuse *(Unisys)*
Klaus Julisch *(IBM Research Zürich)*
Oliver Karow *(Symantec)*
Klaus-Peter Kossakowski *(Presecure)*
Hartmut König *(BTU Cottbus)*
Heiko Krumm *(Uni Dortmund)*
Christopher Krügel *(UCSB, Kalifornien)*
Holger Mack *(Secorvo)*
Michael Meier (Vorsitz) *(BTU Cottbus)*
Jens Nedon *(Consecur)*
Christian Schmid *(Linz, Österreich)*
Morton Swimmer *(IBM Research Zürich)*
Stefan Strobel *(Cirosec)*
Marco Thorbrügge *(DFN-CERT)*
Andreas Wespi *(IBM Research Zürich)*
Stephen Wolthusen *(Fraunhofer IGD Darmstadt)*
Ralf Zessin *(Maxpert AG)*

Sponsoren

dortmund-project

Horst Görtz Institut
für Sicherheit in der Informationstechnik

Logo-Gestaltung

"DIMVA 2004" Logo:
Loom-IT GmbH

DIMVA 2004 Workshop-Programm DIMVA 2004 Workshop-Programm DIMVA 2004 Workshop-Programm DIMVA 2004 Workshop-P

Gesellschaft für Informatik e.V.
Fachgruppe SIDAR

DIMVA 2004

Detection of Intrusions and Malware
& Vulnerability Assessment

6.-7. Juli 2004 | Dortmund

http://www.gi-fg-sidar.de/dimva2004/
mailto: dimva2004@gi-fg-sidar.de

In Kooperation mit:

acm German Chapter
IEEE

Anmeldung und Anreise

Gebühren und Anmeldung

Teilnahmegebühren:

	Bei Zahlungseingang... bis 1.6.2004	ab 2.6.2004
Reguläre Gebühr	265 €	315 €
GI-Mitglieder	175 €	225 €
Studierende/Auszubildende	60 €	80 €
student./auszub. GI-Mitglieder	30 €	50 €

Die reguläre Teilnahmegebühr enthält den Tagungsband, eine Führung durch die Deutsche Arbeitsschutzausstellung (DASA), Pausenerfrischungen, zwei Mittagsbuffets sowie ein Abendbuffet.

Begleitpersonen und Studierende können zur Teilnahme am Abendbuffet ein Ticket zu **40€** erwerben.

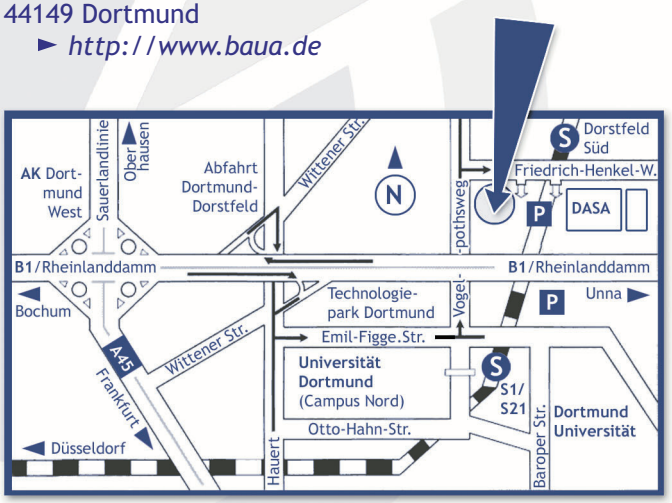
Anmeldeformular und Anreiseinformation:
Bitte beziehen Sie das Anmeldeformular und die Informationen zur Anreise über die Website des Workshops:

► *http://www.gi-fg-sidar.de/dimva2004/*

Anreise

Veranstaltungsort:
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin
Friedrich-Henkel-Weg 1-25
44149 Dortmund

► *http://www.baua.de*



Veranstaltungsprogramm

Dienstag, 6. Juli 2004

Tagesthema: "Intrusion Detection" Entdeckung von Schutzzielverletzungen

8:30 - 9:45 Uhr:
Anmeldung und Erfrischungen

9.45 - 10.00 Uhr:
Begrüßung

10.00 - 11.00 Uhr:
Keynote: Verfahren der Transaktionsanalyse am Beispiel der Missbrauchsfrüherkennung im Kreditkartengeschäft
Hanns-Michael Hepp (Intelligent Risk Solutions)

11.30 - 12.30 Uhr:
Alarm Reduction and Correlation in Intrusion Detection Systems
Tobias Chyssler, Kalle Burbeck (University of Linköping, SE), Stefan Burschka, Michael Semling, Tomas Lingvall (Swisscom, CH)

Alert Verification - Determining the Success of Intrusion Attempts
Christopher Kruegel, William Robertson (University of California, Santa Barbara, USA)

12.30 - 14.00 Uhr:
Pause mit Mittagsbuffet

14.00 - 15.30 Uhr:
Komponenten für kooperative Intrusion-Detection in dynamischen Koalitionsumgebungen
Marko Jahnke, Martin Lies, Michael Bussmann, Sven Henkel (FGAN), Jens Tölle (Universität Bonn)

Vertrauensbasierte Laufzeitüberwachung verteilter komponentenstrukturierter E-Commerce-Software
Peter Herrmann, Heiko Krumm (Universität Dortmund), Lars Wiebusch (E-Plus Mobilfunk)

Intrusion detection in unlabeled data with quarter-sphere Support Vector Machines
Pavel Laskov, Christin Schäfer (Fraunhofer-FIRST), Igor Kotenko (SPIIRAS, RU)

16.00 - 17.00 Uhr:
Sensors for Detection of Misbehaving Nodes in MANETs
Frank Kargl, Andreas Klenk, Michael Weber, Stefan Schlott (Universität Ulm)

Aktive Strategien zur Schutzzielverletzungserkennung durch eine kontrollierte Machtteilung in der Zugriffskontrollarchitektur
Joerg Abendroth (Trinity College Dublin, IE)

17.15 - 19.00 Uhr:
Sitzung der GI-Fachgruppe SIDAR

19.00 - 24.00 Uhr:
Sektempfang und Abendbuffet (in der Stahlhalle der DASA)

Mit markierte Beiträge werden in englischer Sprache veröffentlicht. Die Autoren sind frei, Ihre Beiträge in englischer oder in deutscher Sprache zu präsentieren.

Veranstaltungsprogramm

Mittwoch, 7. Juli 2004

Tagesthema: Verwundbarkeiten und Agenten mit Schadensfunktion

8.30 - 9.00 Uhr:
Anmeldung und Erfrischungen

9.00 - 10.30 Uhr:
Ein Ansatz zur Intrusion Detection für Prozessautomatisierungssysteme
Martin Naedele (ABB Corporate Research, CH)

Visual-IDS oder eine andere Sicht der Dinge
Andreas und Daniela Lindenblatt, Björn Scheuermann (Solution)

Foundations for Intrusion Prevention
Shai Rubin, Ian D. Alderman, David W. Parter, Mary K. Vernon (University of Wisconsin, USA)

11.00 - 12.30 Uhr:
A Honeynet within the German Research Network - Experiences and Results
Helmut Reiser (Ludwig Maximilian Universität München), Gereon Volker (Technische Universität München)

Ermittlung von Verwundbarkeiten mit elektronischen Ködern
Maximilian Dornseif (Universität Bonn), Felix C. Gärtner, Thorsten Holz (RWTH Aachen)

Ein Netzwerk von IDS-Sensoren für Angriffsstatistiken
Olaf Gellert, Till Dörges, Klaus-Peter Kossakowski (Presecure)

12.30 - 14.00 Uhr:
Pause mit Mittagsbuffet

14.00 - 16.00 Uhr:
Structural Comparison of Executable Objects
Halvar Flake

Anti-Patterns in JDK Security and Refactorings
Marc Schönefeld (Universität Bamberg)

Hardened OS exploitation techniques
Sebastian Krahmer (SuSE)

UNIX und Linux basierte Kernel Rootkits
Andreas Bunten (DFN-CERT)

16.30 - 17.30 Uhr:
LIV - The Linux Intregrated Viruswall
Teobaldo A. Dantas de Medeiros (Federal Center for Technological Education, BR), Paulo S. Motta Pires (University of Rio Grande, BR)

Risiken der Nichterkennung von Malware in komprimierter Form
Heiko Fangmeier, Michel Messerschmidt, Fabian Müller, Jan Seedorf (antiVirusTestCenter)

17.30 - 17.45 Uhr:
Verabschiedung