DIMVA 2004

Detection of Intrusions and Malware & Vulnerability Assessment

6.-7. Juli 2004 • Dortmund, Deutschland

Gebäude 1 der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin
Friedrich Henkel-Weg 1-25, 44149 Dortmund

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

Workshop-Überblick

Dienstag 06.07.2004

08.30 - 09.45 Uhr:	Anmeldung
09.45 - 10.00 Uhr:	Begrüßung
10.00 - 11.00 Uhr:	Keynote
11.00 - 11.30 Uhr:	Pause
11.30 - 12.30 Uhr:	Sektion 1: Intrusion Detection I
12.30 - 14.00 Uhr:	Mittagsbuffet
14.00 - 15.30 Uhr:	Sektion 2: Intrusion Detection II
15.30 - 16.00 Uhr:	Pause
16.00 - 17.00 Uhr:	Sektion 3: Intrusion Detection III
17.15 - 19.00 Uhr:	Sitzung der GI-Fachgruppe SIDAR
19.00 - 24.00 Uhr:	Abendbuffet in der DASA

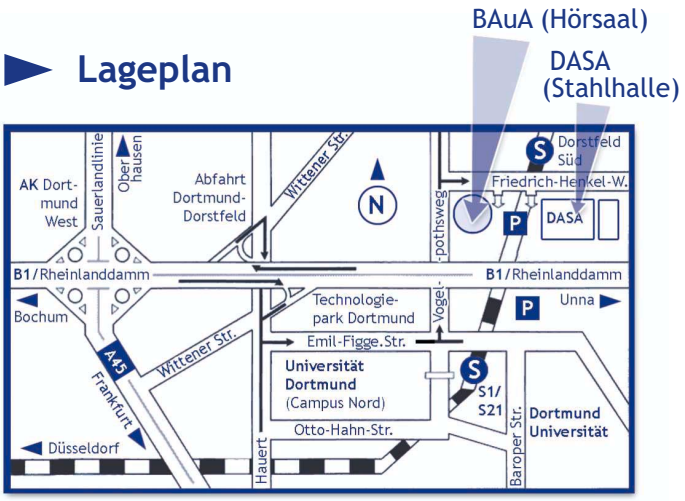
Führungen durch die DASA:

17:30 - 18:30 Uhr:	Beginn am Eingang der DASA
21:00 - 22:00 Uhr:	Beginn in der Stahlhalle der DASA
21:30 - 22:30 Uhr:	Beginn in der Stahlhalle der DASA

Mittwoch 07.07.2004

08.30 - 09.00 Uhr:	Anmeldung
09.00 - 10.30 Uhr:	Sektion 4: Intrusion Detection IV
10.30 - 11.00 Uhr:	Pause
11.00 - 12.30 Uhr:	Sektion 5: Ködersysteme
12.30 - 14.00 Uhr:	Mittagsbuffet
14.00 - 16.00 Uhr:	Sektion 6: Verwundbarkeiten
16.00 - 16.30 Uhr:	Pause
16.30 - 17.30 Uhr:	Sektion 7: Malware
17.30 - 17.45 Uhr:	Verabschiedung

Lageplan



Mit freundlicher Unterstützung

dortmund-project

Horst Görtz Institut für Sicherheit in der Informationstechnik

Organisatorisches

Die Vorträge finden im Hörsaal von Gebäude 1 der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) statt.

Die Pausenerfrischungen und die Mittagsbuffets werden am 6. und 7. Juli im Hörsaal-Foyer der BAuA angeboten. Alle Teilnehmer möchten bitte ihre Teilnehmerschilder sichtbar tragen, da diese zum Bezug von Erfrischungen und zur Teilnahme an den Mittagsbuffets berechtigen.

Sektempfang und Abendbuffet finden am 6. Juli in der Stahlhalle der Deutschen Arbeitsschutzausstellung (DASA) statt. Alle Teilnehmer und Begleitpersonen möchten hierzu bitte ihr persönliches Dinner-Ticket mitbringen.

Vorsitzender der Tagung:
Ulrich Flegel, *Universität Dortmund*

Vorsitzender des Programmkomitees:
Michael Meier, *Brandenburgische Techn. Universität Cottbus*

Tagungsbüro und lokale Organisation:
Claudia Graute, Elke Herrmann, Frank Müller, Sandra Wortmann, *Universität Dortmund*

Programmkomitee:
Thomas Biege, *SuSE Linux AG*
Roland Büschkes, *T-Mobile*
Toralv Dirro, *Network Associates*
Anja Feldmann, *TU München*
Ulrich Flegel, *Universität Dortmund*
Christian Freckmann, *TÜV-IT*
Oliver Göbel, *RUS-CERT*
Christian Götz, *Cirosec*
Dirk Häger, *BSI*
Marc Heuse, *n.runs*
Klaus Julisch, *IBM Research Zürich*
Oliver Karow, *Symantec*
Klaus-Peter Kossakowski, *Presecure*
Hartmut König, *BTU Cottbus*
Heiko Krumm, *Universität Dortmund*
Christopher Krügel, *UCSB, Kalifornien*
Holger Mack, *Secorvo*
Michael Meier, *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, *FhG IGD Darmstadt*
Ralf Zessin, *Maxpert AG*

Veranstalter:
Fachgruppe SIDAR der Gesellschaft für Informatik e.V.

DIMVA 2004

Detection of Intrusions and Malware & Vulnerability Assessment

6.-7. Juli 2004 • Dortmund, Deutschland

Workshop-Programm

Dienstag, 6. Juli 2004

08:30 - 09:45 Uhr: **Anmeldung und Erfrischungen**

09.45 - 10.00 Uhr: **Begrüßung**
Ulrich Flegel, Michael Meier

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

11:00 - 11:30 Uhr: **Pause mit Erfrischungen**

11.30 - 12.30 Uhr: **Sektion 1 - "Intrusion Detection I"**
Moderation: Roland Büschkes (T-Mobile, DE)

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 Krügel, William Robertson (University of California, Santa Barbara, USA)

12.30 - 14.00 Uhr: **Pause mit Mittagsbuffet**

14.00 - 15.30 Uhr: **Sektion 2 - "Intrusion Detection II"**
Moderation: Christopher Krügel (UCSB, USA)

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

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

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

15:30 - 16:00 Uhr: **Pause mit Erfrischungen**

16.00 - 17.00 Uhr: **Sektion 3 - "Intrusion Detection III"**
Moderation: Klaus Julisch (IBM Research, CH)

Sensors for Detection of Misbehaving Nodes in MANETs
Frank Kargl, Andreas Klenk, Michael Weber, Stefan Schlott (Universität Ulm, DE)

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**
Moderation: Klaus-Peter Kossakowski (Presecure, DE)

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

Parallel: **Führungen durch die Deutsche Arbeitsschutz-Ausstellung (DASA)**
17:30 - 18:30 Uhr
Eingang DASA
21:00 - 22:00 Uhr
Stahlhalle DASA
21:30 - 22:30 Uhr
Stahlhalle DASA

Mittwoch, 7. Juli 2004

08.30 - 09.00 Uhr: **Anmeldung und Erfrischungen**

09.00 - 10.30 Uhr: **Sektion 4 - "Intrusion Detection IV"**
Moderation: Stephen Wolthusen (FHG IGD, DE)

Ein Ansatz zur Intrusion Detection für Prozessautomatisierungssysteme
Martin Naedele (ABB Corporate Research, CH)

V-IDS oder eine andere Sicht der Dinge
Björn Scheuermann, Andreas Lindenblatt, Daniela Lindenblatt, Benjamin Guthier (Solution, DE)

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

10.30 - 11.00 Uhr: **Pause mit Erfrischungen**

11.00 - 12.30 Uhr: **Sektion 5 - "Ködersysteme"**
Moderation: Heiko Krumm (Universität Dortmund, DE)

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

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

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

12.30 - 14.00 Uhr: **Pause mit Mittagsbuffet**

14.00 - 16.00 Uhr: **Sektion 6 - "Verwundbarkeiten"**
Moderation: Marc Heuse (n.runs, DE)

Structural Comparison of Executable Objects
Halvar Flake (DE)

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

Hardened OS exploitation techniques
Sebastian Krahmer (SuSE, DE)

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

16.00 - 16.30 Uhr: **Pause mit Erfrischungen**

16.30 - 17.30 Uhr: **Sektion 7 - "Malware"**
Moderation: Toralv Dirro (Network Associates, DE)

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, DE)

17.30 - 17.45 Uhr: **Verabschiedung**
Ulrich Flegel, Michael Meier

19.00 Uhr: **Sitzung des Programmkomitees**