Organisation

Office

Christiane Tronigger
NetHotels Reisebüro Betrieb-GmbH
Neulinggasse 31,
A-1080 Vienna, Austria
Tel.: (+43-1)710 19 19, Fax.: (+43-1)710 19 20
► *dimva2005@gi-fg-sidar.de (General Questions)*
office@nethotels.com (Registration, Hotel)

Organisation Committee

Christopher Kruegel *(Conference Chair)*
Technical University Vienna,
Institut für Rechner gestützte Automation,
Treitlstraße 3/4. Stock, A-1040 Vienna, Austria
Tel.: (+43-1)58 801-183 25, Fax.: (+43-1)58 801-183 91
► *chris@auto.tuwien.ac.at*

Klaus Julisch *(Program Committee Chair)*
IBM Research GmbH,
Säumerstrasse 4,
CH-8803 Rüschlikon, Switzerland
Tel.: (+41-44)724 8608, Fax.: (+41-44)724 8953
► *kju@zurich.ibm.com*

Organiser

Special Interest Group SIDAR
German Informatics Society (GI)
Wissenschaftszentrum, Ahrstraße 45,
D-53175 Bonn, Germany
Tel.: (+49-228)302-145, Fax: (+49-228)302-167
► *http://www.gi-ev.de*

In cooperation with:
IEEE Computer Society Technical Committee on Security and Privacy
IEEE Task Force on Information Assurance

Logo-Design

“DIMVA 2005” Logo:
Loom-IT GmbH

Organisation

Steering Committee

Members:

Ulrich Flegel, *University of Dortmund, Germany*
Michael Meier, *Technical University of Cottbus, Germany*

Roland Büschkes, *T-Mobile, Germany*
Marc Heuse, *n.runs, Germany*

Program Committee

Members:

Dominique Alessandri (*IBM, Switzerland*)
Thomas Biege (*SUSE LINUX AG, Germany*)
Roland Büschkes (*T-Mobile, Germany*)
Marc Dacier (*Institut Eurécom, France*)
Herve Debar (*France Telecom R&D, France*)
Luca Deri (*ntop.org, Italy*)
Sven Dietrich (*CMU, USA*)
Toralv Dirro (*McAfee, Germany*)
Ulrich Flegel (*University of Dortmund, Germany*)
Steven Furnell (*University of Plymouth, UK*)
Detlef Günther (*CERT-VW, Germany*)
Dirk Häger (*BSI, Germany*)
Bernhard Hämmerli (*HTA Luzern, Switzerland*)
Oliver Heinz (*arago AG, Germany*)
Peter Herrmann (*University of Dortmund, Germany*)
Marc Heuse (*n.runs, Germany*)
Erland Jonsson (*Chalmers University of Technology, Sweden*)
Engin Kirda (*Vienna University of Technology, Austria*)
Hartmut König (*Technical University of Cottbus, Germany*)
Klaus-Peter Kossakowski (*Presecure, Germany*)
Hannes Lubich (*Computer Associates, Switzerland*)
Michael Meier (*Technical University of Cottbus, Germany*)
Martin Naedele (*ABB Corporate Research, Switzerland*)
Marc Rennhard (*ETH Zurich, Switzerland*)
Dirk Schadt (*Computer Associates, Germany*)
Robin Sommer (*Technical University Munich, Germany*)
Axel Tanner (*IBM Research, Switzerland*)
Stephen Wolthusen (*Fraunhofer-IGD, Germany*)

DIMVA 2005 Conference Program DIMVA 2005 Conference Program DIMVA 2005 Conference Program DIMVA 2005

German Informatics Society
Special Interest Group SIDAR

DIMVA 2005

Detection of Intrusions and Malware
& Vulnerability Assessment

7-8 July 2005 | Vienna, Austria

http://www.dimva.org/dimva2005/
mailto: dimva2005@gi-fg-sidar.de

In cooperation with:
IEEE

Registration Information

Conference Fees:

	When payment ... until 1.6.2005	after 1.6.2005
Regular Fee	295 €	345 €
Fee for GI-Members	195 €	245 €
Student Fee	75 €	90 €

The conference fees include:

- Access to all technical presentations.
- Copy of conference proceedings.
- Admission to the conference reception (additional tickets can be purchased at the conference).
- Lunch and refreshments on both days.
- Conference gifts.

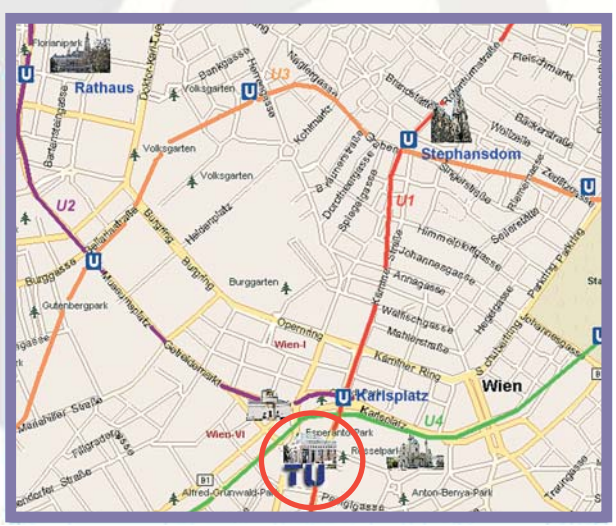
Registration and Travel Information:
To register online, please visit the conference web site. There, you will also find travel information and links to hotels with special rates for conference attendees.

► *http://www.dimva.org/dimva2005/*

Conference Location:
Freihaus (Hoersaal 6), Technical University Vienna
Wiedener Hauptstraße 8-10, A-1040 Vienna, Austria

► *http://www.tuwien.ac.at*

Map



From Thursday, 7. July 2005 ...

8.30 - 9.45
Registration

9.45 - 10.00
Welcome

10.00 - 11.00: Keynote
Philip Attfield (Northwest Security Institute)

11.30 - 12.30: Obfuscated Code Detection
Analyzing Memory Accesses in Obfuscated x86 Executables
Michael Venable, Mohamed Chouchane, Md Enamul Karim, & Arun Lakhotia
Hybrid Engine for Polymorphic Shellcode Detection
Udo Payer, Peter Teufl, & Mario Lamberger

12.30 - 14.00
Lunchbreak

14.00 - 15.00: Honeypots
Experiences Using Minos as a Tool for Capturing & Analyzing Novel Worms for Unknown Vulnerabilities
Jedidiah R. Crandall, S. Felix Wu, & Frederic T. Chong
A Pointillist Approach for Comparing Honeypots
Fabien Pouget & Thorsten Holz

15.30 - 17.00: Vulnerability Assessment and Exploit Analysis
Automatic Detection of Attacks on Cryptographic Protocols: A Case Study
Ivan Cibrario B., Luca Durante, Riccardo Sisto, & Adriano Valenzano
METAL - A Tool for Extracting Attack Manifestations
Ulf Larson, Emilie Lundin-Barse, & Erland Jonsson
Flow-Level Traffic Analysis of the Blaster & Sobig Worm Outbreaks in an Internet Backbone
Thomas Dübendorfer, Theus Hossmann, Arno Wagner, & Bernhard Plattner

17.00 - 18.30
Meeting of GI - Special Interest Group SIDAR

19.00 - 24.00: Reception
Festsaal of the Town Hall of Vienna
(including a guided tour through the Town Hall)

Conference Program

... until Friday, 8. July 2005

9.30 - 11.00: Anomaly Detection
A Learning-Based Approach to the Detection of SQL Attacks
Fredrik Valeur, Darren Mutz, & Giovanni Vigna
Masquerade Detection via Customized Grammars
Mario Latendresse
A Prevention Model for Algorithmic Complexity Attacks
Suraiya Khan & Issa Traore

11.30 - 12.30: Misuse Detection
Detecting Malicious Code by Model Checking
Johannes Kinder, Stefan Katzenbeisser, Christian Schallhart, & Helmut Veith
Improving the Efficiency of Misuse Detection
Michael Meier, Sebastian Schmerl, & Hartmut Koenig

12.30 - 14.00
Lunchbreak

14.00 - 15.00: Distributed Intrusion Detection and Testing
Enhancing the Accuracy of Network-based Intrusion Detection with Host-based Context
Holger Dreger, Christian Kreibich, Vern Paxson, & Robin Sommer
TCPtransform: Property-Oriented TCP Traffic Transformation
Seung-Sun Hong, Fiona Wong, S. Felix Wu, Bjorn Lilja, Tony Y. Jansson, Henric Johnson, & Arne Nelsson

15.30 - 17.00: Industry Session
Implementation of Honeytoken Module in DBMS Oracle 9iR2 Enterprise Edition for Internal Malicious Activity Detection
Antanas Cenys, Darius Rainys, Lukas Radvilavicius, & Nikolaj Goranin
Function Call Tracing Attacks To Kerberos 5
Julian Rrushi & Emilia Rosti
Combining IDS and Honeynet Methods for Improved Detection and Automatic Isolation of Compromised Systems
Stephan Riebach, Birger Toedtmann, & Erwin Rathgeb

17.00 - 17.15
Closing Remarks