Welcome to

# DIMVA 2010

## July 08+09 2010
## Bonn, Germany

Organized by the GI Special Interest Group SIDAR

Fraunhofer

FKIE

universität**bonn**

- **Bonn at the River Rhine**
  – former capital of Germany

- Famous for science & education, music, politics, and industrial global player's headquarters

- More info: http://www.bonn.de

DIMVA 2010

Pictures © wikipedia.de

- **Gold Sponsor**

- Sponsors

# DIMVA 2010 – Conference Facilities

- Location: **Centre of Sciences** (Wissenschaftszentrum)
- Lobby
  - Conference desk
  - Restrooms
  - Coffee breaks
  - Light Lunch (Thursday)
- Cafeteria
  - Full Lunch (Friday)
- Souterrain
  - German technical museum



Pictures © Wissenschaftszentrum Bonn

- Please switch off mobile phones in conference room. Thank you.
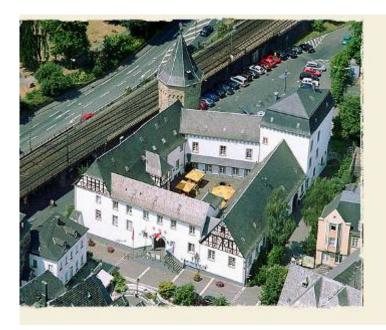


- WiFi / WLAN available.
    - ESSID:
    - Username:
    - Password:

# DIMVA 2010 – Social Event Tonight

- **Knight's dinner** at the **Castle of Linz**, ~20km from Bonn
- Transport, entertainment & dinner (lots of meat!)
- Rustic environment – robust clothing, please ;-)
- Vouchers for transport/meal
- Buses from/to conference location
    - Departure from Wissenschaftszentrum:        **18:30**
    - Departure from Linz Castle:                          approx. **22:30**



Pictures © Linz Castle

## Peter Martini

Head of Fraunhofer FKIE
and Institute of
Computer Science 4,
University of Bonn

# DIMVA 2010 – Welcome from PC Chair

## Program Committee

- **Michael Bailey**, University of Michigan, USA
- **Herbert Bos**, Vrije Universiteit Amsterdam, Netherlands
- **Juan Caballero**, CMU/UC Berkeley, USA
- **Hervé Debar**, Télécom SudParis, France
- **Sven Dietrich**, Stevens Institute of Technology, USA
- **Holger Dreger**, Siemens CERT, Germany
- **Ulrich Flegel**, SAP Research, Germany
- **Carrie Gates**, CA Labs, USA
- **Chris Grier**, University of California, Berkeley, USA
- **Guofei Gu**, Texas A&M University, USA
- **Thorsten Holz**, Vienna University of Technology, Austria
- **Piotr Kijewski**, NASK/CERT Polska, Poland
- **Engin Kirda**, Eurecom, France
- **Christopher Kruegel**, University of California, Santa Barbara, USA

- **Wenke Lee**, Georgia Institute of Technology, USA.
- **Corrado Leita**, Symantec Research Labs, France
- **Kirill Levchenko**, University of California, San Diego, USA
- **Pavel Laskov**, University of Tuebingen, Germany
- **Ludovic Me**, Supelec, France
- **Michael Meier**, Technical University of Dortmund, Germany
- **Tyler Moore**, Harvard University, USA
- **Lexi Pimenidis**, iDev GmbH, Germany
- **Moheeb Rajab**, Google/Johns Hopkins University, USA
- **Sebastian Schmerl**, BTU Cottbus, Germany
- **Robin Sommer**, ICSI/LBNL, USA
- **Henry Stern**, Cisco/Ironport, USA
- **Diego Zamboni**, IBM Research, Switzerland

# DIMVA 2010 – Preliminary Statistics

- Registered participants:          86 (from 16 countries)
    - Academia
    - Research
    - Industry
    - Public authorities
    - Students
    - Press


- Submitted papers:          35 (from 19 countries)
- Accepted papers:          12 (acc. rate: 34%)

## Thursday, July 08

| | |
|---|---|
| 09:00-09:15 | **Welcome** |
| 09:15-10:30 | **Keynote**<br>Trends in Malevolence<br>*Jose Nazario*<br>Arbor Networks |
| 10:30-11:00 | **Coffee break** |
| 11:00-12:30 | **Session 1 – Host Security**<br>Session Chair: *Christian Kreibich* |

HookScout: Proactive Binary-Centric Hook Detection
*Heng Yin, Pongsin Poosankam, Steve Hanna and Dawn Song*

Conqueror: Tamper-proof Code Execution on Legacy Systems
*Lorenzo Martignoni, Roberto Paleari and Danilo Bruschi*

dAnubis - Dynamic Device Driver Analysis Based on Virtual Machine Introspection
*Matthias Neugschwandtner, Christian Platzer, Paolo Milani Comparetti and Ulrich Bayer*

| | |
|---|---|
| 12:30-13:30 | **Lunch** |
| 13:30-14:45 | **Invited Talk**<br>Modern Spammer Infrastructure<br>*Carel van Straaten*<br>Spamhaus |
| 14:45-16:00 | **Session 2 – Trends**<br>Session Chair: *Sven Dietrich* |

Evaluating Bluetooth as a Medium for Botnet Command and Control
*Kapil Singh, Samrit Sangal, Nehil Jain, Patrick Traynor and Wenke Lee*

Take a Deep Breath: a Stealthy, Resilient and Cost-Effective Botnet Using Skype
*Antonio Nappa, Aristide Fattori, Marco Balduzzi, Matteo Dell'Amico and Lorenzo Cavallaro*

Covertly Probing Underground Economy Marketplaces
*Hanno Fallmann, Gilbert Wondracek and Christian Platzer*

## Thursday, July 08 (cont'd)

| | |
|---|---|
| 16:00-16:15 | **Coffee break** |
| 16:15-17:15 | **Session 3 – Vulnerabilities** |
| | Session Chair: *Michael Meier* |
| | Why Johnny Can't Pentest: An Analysis of Black-box Web Vulnerability Scanners |
| | *Adam Doupe, Marco Cova and Giovanni Vigna* |
| | Organizing Large Scale Hacking Competitions |
| | Nick Childers, Bryce Boe, Lorenzo Cavallaro, *Ludovico Cavedon, Marco Cova, Manuel Egele and Giovanni Vigna* |
| 17:15-18:15 | Meeting of GI SIG SIDAR (open to all attendees) |
| | Invited Talk: Quo Vadis Sicherheitsausbildung?, *Martin Mink, TU Darmstadt* |
| 18:30 | Bus departure for social event |

# DIMVA 2010 – Friday Program

## Friday, July 09

09:00-10:15 **Invited Talk**
*TRIAGE: the WOMBAT attack attribution approach*
Marc Dacier
Symantec / Eurecom

10:15-10:45 **Coffee break**

10:45-11:45 **Session 4 – Intrusion Detection**
Session chair: *Robin Sommer*

An Online Adaptive Approach to Alert Correlation
*Hanli Ren, Natalia Stakhanova and Ali Ghorbani*

KIDS - Keyed Intrusion Detection System
*Sasa Mrdovic*

11:45-12:30 **Rump Session**
Session chair: *Sven Dietrich*

12:30-13:30 **Lunch**

13:30-14:30 **Session 5 – Web Security**
Session Chair: *Herbert Bos*

Modeling and Containment of Search Worms Targeting Web Applications
*Jingyu Hua and Kouichi Sakurai*

HProxy: Client-side detection of SSL stripping attacks
*Nick Nikiforakis, Yves Younan and Wouter Joosen*

14:30-14:45 **Concluding Remarks**

# Enjoy your stay…

…and in case of any questions,
please meet us at the conference desk.

Fraunhofer

FKIE

universität**bonn**