DIMVA 2010
July 08+09 2010
Bonn, Germany
Organized by the GI Special Interest Group SIDAR
- **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](http://www.bonn.de)
DIMVA 2010 - Thanks to our Sponsors

- Gold Sponsor

- Sponsors

QUALYS

FOA

G DATA
- Location: **Centre of Sciences** (Wissenschaftszentrum)
- Lobby
  - Conference desk
  - Restrooms
  - Coffee breaks
  - Light Lunch (Thursday)
- Cafeteria
  - Full Lunch (Friday)
- Souterrain
  - German technical museum
• 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
DIMVA 2010 - Welcome from Local Host

Peter Martini
Head of Fraunhofer FKIE and Institute of Computer Science 4, University of Bonn
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%)
# DIMVA 2010 - Thursday Program (1/2)

**Thursday, July 08**

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:00-09:15</td>
<td>Welcome</td>
<td></td>
</tr>
<tr>
<td>09:15-10:30</td>
<td>Keynote</td>
<td>Jose Nazario, Arbor Networks</td>
</tr>
<tr>
<td></td>
<td><strong>Trends in Malevolence</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Session Chair:</strong></td>
<td>Sven Dietrich</td>
</tr>
<tr>
<td>10:30-11:00</td>
<td><strong>Coffee break</strong></td>
<td></td>
</tr>
<tr>
<td>11:00-12:30</td>
<td><strong>Session 1 - Host Security</strong></td>
<td>HookScout: Proactive Binary-Centric Hook Detection</td>
</tr>
<tr>
<td></td>
<td><strong>Session Chair:</strong></td>
<td>Christian Kreibich</td>
</tr>
<tr>
<td></td>
<td><strong>HookScout</strong>:</td>
<td>Heng Yin, Pongsin Poosankam, Steve Hanna and Dawn Song</td>
</tr>
<tr>
<td></td>
<td><strong>Conqueror</strong>:</td>
<td>Lorenzo Martignoni, Roberto Paleari and Danilo Bruschi</td>
</tr>
<tr>
<td></td>
<td><strong>dAnubis</strong>:</td>
<td>Matthias Neugschwandtner, Christian Platzer, Paolo Milani Comparetti and Ulrich Bayer</td>
</tr>
<tr>
<td></td>
<td><strong>Session 2 - Trends</strong></td>
<td>Evaluating Bluetooth as a Medium for Botnet Command and Control</td>
</tr>
<tr>
<td></td>
<td><strong>Session Chair:</strong></td>
<td>Sven Dietrich</td>
</tr>
<tr>
<td></td>
<td><strong>Evaluating Bluetooth as a Medium for Botnet Command and Control</strong></td>
<td>Kapil Singh, Samrit Sangal, Nehil Jain, Patrick Traynor and Wenke Lee</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Take a Deep Breath: a Stealthy, Resilient and Cost-Effective Botnet Using Skype</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Antonio Nappa, Aristide Fattori, Marco Balduzzi, Matteo Dell'Amico and Lorenzo Cavallaro</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Covertly Probing Underground Economy Marketplaces</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hanno Fallmann, Gilbert Wondracek and Christian Platzer</td>
</tr>
<tr>
<td>12:30-13:30</td>
<td>Lunch</td>
<td></td>
</tr>
<tr>
<td>13:30-14:45</td>
<td>Invited Talk</td>
<td>Carel van Straaten, Spamhaus</td>
</tr>
<tr>
<td></td>
<td><strong>Modern Spammer Infrastructure</strong></td>
<td></td>
</tr>
<tr>
<td>14:45-16:00</td>
<td>Session 2 - Trends</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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
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.