2009 Fifth International Conference on IT Security Incident Management and IT Forensics

(IMF 2009)

Stuttgart, Germany
15-17 September 2009
Table of Contents
2009 Fifth International Conference on IT Security Incident Management and IT Forensics
IMF 2009

Workshops

Digital Discovery with Bootable CDs
Ralf Moll, Federal Police Baden-Wuerttemberg, Germany,
Michael Prokop, grml Solutions, Austria, Holger Morgenstern, gutachten.info, Germany

Keynotes

Thilo Weichert
Privacy Commissioner of Schleswig-Holstein, Germany
Independent Centre for Privacy Protection Schleswig-Holstein, Germany

Overcast: Forensic Discovery in Cloud Environments .............................................. 3
Stephen D. Wolthusen, Royal Holloway, University of London, UK

Presentations

Experiences with the NoAH Honeynet Testbed to Detect new Internet Worms............... 13
Jan Kohlrausch

Botnet Statistical Analysis Tool for Limited Resource Computer Emergency Response Team.........27
Kamol Kaemarungsri, Nawattapon Yoskamtorn, Kitisak Jirawannakool, Nuttapon Sanglerdsinlapachai, and Chanin Luangkingkasut

Semi-autonomous Link Layer Vulnerability Discovery and Mitigation Dissemination ............ 41
Ziyad Al-Salloum and Stephen Wolthusen

From the Computer Incident Taxonomy to a Computer Forensic Examination Taxonomy .......... 54
Robert Altschaffel, Stefan Kiltz, and Jana Dittmann
Fast User Classifying to Establish Forensic Analysis Priorities ................................................................. 69
  Antonio Grillo, Alessandro Lentini, Gianluigi Me, and Matteo Ottoni

The Forensic Image Generator Generator (Forensig2) ................................................................................. 78
  Christian Moch and Felix C. Freiling

  Rafael Accorsi

Technique to Interrogate an Image of RAM111 .............................................................................................. 111
  Mark Wozar

An Automated User Transparent Approach to log Web URLs for Forensic Analysis ............................... 120
  Muhammad Kamran Ahmed, Mukhtar Hussain, and Asad Raza

Self-Forensics through Case Studies of Small-to-Medium Software Systems ........................................... 128
  Serguei A. Mokhov and Emil Vassev

Analysis of Download Accelerator Plus (DAP) for Forensic Artefacts ...................................................... 142
  Muhammad Yasin, Muhammad Arif Wahla, and Firdous Kausar

A Comprehensive and Comparative Analysis of the Patching Behavior of Open Source and Closed
Source Software Vendors .......................................................................................................................... 153
  Guido Schryen

Author Index