Preface

Information technology has become crucial to almost every part of society. IT infrastructures are critical to the world-wide economy, the financial sector, the health sector, the government’s administration, the military, and the educational sector. Due to its importance the disruption or loss of IT capabilities results in a massive reduction of operability.

Hence, IT security is continuously gaining importance and has become technically essential to IT infrastructures.

Although security usually gets integrated into the design process of IT systems nowadays, the process of maintaining security in IT infrastructure operation still lacks the appropriate attendance in most cases.

Especially the capability to manage and respond to IT security incidents and their forensic analysis is established in the rarest cases. The quickly rising number of security incidents worldwide makes the implementation of incident management capabilities, targeting the mitigation of immediate consequences to the own infrastructure, essential.

Also, the need of subsequent forensic analysis of selected cases to gather evidence on the incident’s details and work up the information for law suits or to avert unwarranted liability claims of aggrieved third parties is constantly growing.

In order to advance the fields of IT-Incident Management and IT-Forensics the special interest group Security - Intrusion Detection and Response (SIDAR) of the German Informatics Society (GI) organises the annual International Conference on IT-Incident Management and IT-Forensics (IMF), bringing together experts from throughout the world, to discuss state of the art in these areas. IMF promotes collaboration and exchange of ideas between industry, academia, law-enforcement and other government bodies.

IMF 2006 is supported with keynotes by the German Federal Ministry of the Interior (BMI) and the US National Institute of Standards and Technology (NIST).

The organising committee would like to thank all persons who helped in realising the conference, especially the authors whose papers and presentations make the essence of the conference, the members of the program committee who reviewed and evaluated the papers submitted and whose professional competence ensures the scientific quality of the program, as well as the sponsors who supported the conference.

Oliver Göbel, Sandra Frings, Detlef Günther, Hardo Hase Jens Nedon and Dirk Schadt
Program Committee

Henrik Becker Kanzlei Becker, Germany
Vlasti Broucek University of Tasmania, Australia
Ian Bryant NISCC, UK
Brian Carrier CERIAS, USA
Andrew Cormack UKERNA, UK
Herve Debar France Telecom, France
Ralf Dörrie Telekom CERT, Germany
Maximilian Dornseif University of Mannheim, Germany
Ulrich Emmert esb Rechtsanwälte Stuttgart, Germany
Günther Ennen BSI/CERT-Bund, Germany
Christoph Fischer BFK-Consulting, Germany
Sandra Frings Fraunhofer IAO, Germany
Oliver Göbel RUS-CERT, Universität Stuttgart, Germany
Dieter Gollmann TU Hamburg-Harburg, Germany
Detlef Günther Cert-VW, Volkswagen AG, Germany
Bernhard Hämmerli ACRIS GmbH, Switzerland
Hardo G. Hase, IT-Consulting Hardo G. Hase, Germany
Mark Hoekstra IT Forensic BV, Netherlands
Klaus Peter Kossakowski, DFN-CERT, Germany
Thorsten Lieb Avocado Rechtsanwälte Frankfurt, Germany
Jim Lyle NIST CFTT, USA
Neil Mitchison Joint Reseach Centre, EU
Jens Nedon Consecur GmbH, Germany
Jason Rafail CERT/CC, USA
Damir Rajnovic CISCO-PSIRT, USA
Gavin Reid CISCO/INFOSEC, USA
Dirk Schadt CA, Germany
Christian Schaller SIEMENS-CERT,
Germany Rolf Schulz gnsec, Germany
Marco Thorbruegge ENISA, EU
Helmut Ujen Bundeskriminalamt, Germany
Andreas Wagner Frontrunner FZ LLC, Dubai
Stephen Wolthusen Gjovik University College, Norway
Organising Committee

General chair:        Dirk Schadt, CA, Germany
                      Hardo G. Hase, IT-Consulting Hardo G. Hase, Germany
                      Sandra Frings, Fraunhofer IAO, Germany
                      Oliver Göbel, RUS-CERT, Universität Stuttgart, Germany
                      Detlef Günther, Volkswagen AG, Germany
                      Jens Nedon, Consecur GmbH, Germany

Program Chair:       Oliver Göbel, RUS-CERT, Universität Stuttgart, Germany,
                      goebel @ cert.uni-stuttgart.de

Sponsor Chair:       Dirk Schadt, CA, Germany,
                      dirk.schadt @ gmail.com
Keynotes

Dr. Stefan Grosse
Bundesministerium des Inneren (BMI)
der Bundesrepublik Deutschland

James R. Lyle
National Institute of Standards and Technology (NIST)

The Contribution of Tool Testing to the Challenge of Responding to an IT Adversary

Invited Speaker

Andrea Rigioni
Symantec Corp.

Incident Response and the Role of External Services
# Table of Contents

The Contribution of Tool Testing to the Challenge of Responding to an IT Adversary (Keynote)  
(Jim Lyle) ................................................................. 6

Incident Response and the Role of External Services (Invited Speech)  
(Andrea Rigioni) .......................................................... 14

Technical Development of Cyber Crime  
(Rolf Schulz) ............................................................... 23

Establishing a Centre for Information Security: Experiences from the Trial Period and Recommendations to Similar Initiatives  
(Maria B. Line, Lillian Røstad) ........................................... 43

CarmentIS: A Co-Operative Approach Towards Situation Awareness and Early Warning for the Internet  
(Bernd Grobauer, Jens Ingo Mehlau, Jürgen Sander) ..................... 55

Effectiveness of Proactive CSIRT Services  
(Johannes Wiik, Jose J. Gonzalez, Klaus-Peter Kossakowski) ............. 67

A Distributed Security Announcement Authoring System with CAIF Support  
(Anselm R. Garbe, Oliver Goebel) ........................................ 82

Automated Resolving of Security Incidents as a Key Mechanism to Fight Massive Infections of Malicious Software  
(Jochen Kaiser, Alexander Vitzthum, Peter Holleck, Falco Dressler) ........ 92

Pool Allocations as an Information Source in Windows Memory Forensics  
(Andreas Schuster) ...................................................... 104

A Comparative Study of Teaching Forensics at a University Degree Level  
(Philip Anderson, Maximilian Dornseif, Felix C. Freiling, Thorsten Holz, Alastair Irons, Christopher Laing, Martin Mink) ............ 116

Monitoring of Incident Response Management Performance  
(Maria B. Line, Eirik Albrechtsen, Stig Ole Johnsen, Odd Helge Longva, Stefanie Hillen) ................................................... 128

Detecting New Patterns of Attacks – Results and Applications of Large Scale Sensing Networks  
(Thorsten Voss, Klaus-Peter Kossakowski) .................................. 144