German
Informatics
Society

Preamble

Information technology has become crucial to almost every part of society. IT infrastructures have become critical in 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 result in a massive reduction of operability. Hence, IT security is gaining importance continuously.

Although security usually gets involved into the design process of IT systems nowadays, the process of maintaining security in the operation of IT infrastructures still lacks the appropriate attendance in the most cases. Especially the capability to manage and respond to IT security incidents and their forensic analysis are established in the scarcest cases. The quickly rising number of security incidents worldwide make the implementation of incident management capabilities essential.

In order to advance the fields of IT-Incident Management and Forensics the special interest-group Security - Intrusion Detection and Response (SIDAR) of the German Informatics Society (GI) organises an annual conference in co-operation with Stuttgart University's Computer Emergency Response Team (RUS-CERT) and the Fraunhofer Institute for Industrial Engineering (IAO), bringing together experts from throughout the world, to discuss the state of the art in the areas of Incident Management and IT-Forensics (IMF). IMF promotes collaboration and exchange of ideas between industry, academia, law-enforcement and other government bodies.

Conference Location

University of Stuttgart
Pfaffenwaldring 9
Lecture Hall 9.01
70569 Stuttgart-Vaihingen
Germany

Registration

www.imf-conference.org/imf2007/registration.html

Program Committee

Susan Brenner	University of Dayton, USA
Klaus Brunnstein	University of Hamburg, Germany
Brian Carrier	Basis Technology, USA
Jack Cole	US Army Research Laboratory, USA
Andrew Cormack	UKERNA, UK
Ralf Doerrie	Telekom-CERT, Germany
Sandra Frings	Fraunhofer IAO, Germany
Oliver Goebel	RUS-CERT, Germany
Dieter Gollmann	TU Hamburg-Harburg, Germany
Detlef Guenther	CERT-VW, Volkswagen AG, Germany
Bernhard Haemmerli	ACRIS GmbH, Switzerland
Hardo G. Hase	IT-Security Expert, Germany
Alexander Herrigel	Schweizerische Nationalbank, Switzerland
Thorsten Lieb	Avocado Rechtsanwälte, Germany
Klaus Peter Kossakowski	DFN-CERT, Germany
Jim Lyle	NIST CFTT, USA
Robert A. Martin	MITRE Corporation, USA
Neil Mitchison	European Commission
Jens Nedon	Consecur, Germany
Bernhard Otupal	Interpol
Jason Rafail	CERT/CC, USA
Dirk Schadt	SPOT Consulting, Germany
Carlos Solari	Bell Laboratories, USA
Marco Thorbruegge	ENISA, EU
Stephen Wolthusen	Gjovik University College, Norway
Steven Wood	Alste.Technologies GmbH, Germany

Steering Committee IMF

Oliver Goebel	RUS-CERT, University of Stuttgart
Detlef Guenther	CERT-VW, Volkswagen AG
Jens Nedon	Consecur GmbH
Dirk Schadt	SPOT Consulting

General Chair

Oliver Goebel
RUS-CERT, University of Stuttgart
goebel@cert.uni-stuttgart.de

Program Chair

Sandra Frings
Fraunhofer IAO
sandra.frings@iao.fraunhofer.de

Sponsor Chair

Dirk Schadt
SPOT Consulting
dirk.schadt@spot.net

IMF 2007

Third International GI SIG SIDAR
Conference on
IT-Incident Management & IT-Forensics

Stuttgart, Germany
September 11 - 13, 2007

www.imf-conference.org
mailto:imf2007@gi-fg-sidar.de

SIDAR

Security - **I**ntrusion **D**etection **a**nd **R**esponse

German Informatics Society

September 11, 2007

Time	Presentation	Speaker
10:45	Registration	
11:15	Greeting and Introduction	
11:30	Key Note: About the Role of IT Security in the Information Society	Klaus Brunnstein, IFIP President
12:15	A Common Process Model for Incident Response and Computer Forensics	Felix Freiling, University of Mannheim, Bastian Schwittay, Symantec GmbH
13:00	Lunch	
14:00	IT Incident Management and Structured Documentation	Sandra Frings, Fraunhofer Institut für Arbeitswirtschaft und Organisation (IAO)
14:45	Proposal Of A System For Computer-Based Case And Evidence Management	Fritjof Haft, Pascal Hassenpflug, Hans Lecker, Normfall GmbH
15:30	Break	
16:00	Information-Sharing System for Vulnerability Information Dissemination in Large-Scale Organization	Tohru Sato, Jumpei Watase, NTT Information Sharing Platform Laboratories
16:45	End of day 1	
19:00	Social event	

September 12, 2007

Time	Presentation	Speaker
10:00	Greeting	
10:15	Invited Speaker: IT Based Crime: Evidence Collection & Legal Restrictions in Investigating Cases	Jens Gruhl, Oberstaatsanwalt, Staatsanwaltschaft Konstanz
11:00	A Case Study on Constructing a Security Event Management System	Vijay Gurbani, D. L. Cook, L.E. Menten, T.B. Reddington, Bell Laboratories, Alcatel-Lucent
11:45	Taxonomy of Anti-Computer Forensics Threats	Joseph Sremack, Alexandre V. Antonov, LECG
12:30	Lunch	
13:30	Testing Forensic Hash Tools on Sparse Files	Felix Freiling, University of Mannheim, H. D. IIT Kharagpur, M. Dornseif, Hudora GmbH, Germany
14:15	Towards Reliable Rootkit Detection in Live Response	Felix Freiling, University of Mannheim, B. Schwittay, Symantec GmbH
15:00	Break	
15:30	Key Note: The Security Landscape in a Converged IP World	Carlos C. Solari VP, Security Solutions Group Bell Laboratories Alcatel-Lucent
16:15	Conclusion	
16:30	End of day 2	

September 13, 2007 - Workshop Day

Time	Workstream 1	Workstream 2
09:15	Greeting and Introduction	
09:30	Computer Forensics: High-tech tools for a high-tech problem *Steven Wood, Alste Technologies GmbH*	Octave - Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM} *Christian Paulsen, DFN-CERT Services GmbH*
11:00	Break	
11:30	Memory Analysis on the Microsoft Windows Plattform *Andreas Schuster, Deutsche Telekom AG*	Workshop on X.805 - Security architecture for systems providing end-to-end communications *Suhasini Sabnis, Alcatel-Lucent*
13:00	Lunch	
14:00	Virtualisation of forensic Images *Ralf Moll, LKA Baden-Württemberg, Holger Morgenstern, IT-Service / Sachverständigenbüro Morgenstern*	
15:30	End	

In Cooperation with