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.

Although security usually gets involved in the design process of IT systems nowadays, the process of maintaining security in the operation of IT infrastructures, in most cases, still lacks the appropriate attention. The capability to manage and respond to IT security incidents and their forensic analysis are not well established. The quickly rising number of security incidents worldwide makes the implementation of incident management capabilities essential.

In order to advance the fields of IT Security Incident Management and IT Forensics the special interest-group "Security Intrusion Detection and Response" (SIDAR) of the German Informatics Society (GI) organizes an annual conference, providing a platform for experts from throughout the world, to discuss the state of the art in the areas of IT Security Incident Management and IT Forensics (IMF). IMF promotes collaboration and exchange of ideas between industry, academia, law-enforcement and other government bodies.

The IMF conference will be held for the fourth time in 2008. The concept matured from a pure academic event to an academic track section complemented by practical workshops. In addition, IMF has become an important community event. This year IMF starts to travel. The Mannheim University of Cooperative Education (Berufsakademie Mannheim) will host the fourth IMF.

Conference Location

Mannheim University of Cooperative Education
Coblitzweg 1-7
68163 Mannheim
Germany

Registration

www.imf-conference.org/imf2008/registration.html

Program Committee

Susan Brenner	University of Dayton, USA
Klaus Brunnstein	University of Hamburg, Germany
Jack Cole	US Army Research Laboratory, USA
Andrew Cormack	JANET, UK
Ralf Doerrie	Germany
Sandra Frings	Fraunhofer IAO, Germany
Oliver Göbel	RUS-CERT, Germany
Detlef Günther	ISSO, Volkswagen AG, Germany
Vijay K. Gurbani	Bell Laboratories, Alcatel-Lucent, USA
Bernhard Hämmerli	ACRIS GmbH, Switzerland
Alexander Herrigel	Secude Int. AG, Switzerland
Thorsten Lieb	Avocado Rechtsanwälte, Germany
Klaus Peter Kossakowski	DFN-CERT, Germany
Jim Lyle	NIST, USA
Robert A. Martin	MITRE Corporation, USA
Ralf Moll	LKA Baden-Wuerttemberg, Germany
Jens Nedon	ConSecur GmbH, Germany
Henning Pagnia	Berufsakademie Mannheim, Germany
Hartmut Pohl	FH Bonn-Rhein-Sieg, Germany
Jason Rafail	CERT/CC, USA
Dirk Schadt	SPOT Consulting, Germany
Marc Schiller	Statton Security Ltd, UK
Andreas Schuster	Germany
Marco Thorbrügge	ENISA, EU
Stephen Wolthusen	Royal Holloway, Univ. of London, UK
Steven Wood	Alste.Technologies GmbH, Germany

Steering Committee IMF

Sangra Frings	Fraunhofer IAO
Oliver Göbel	RUS-CERT, University of Stuttgart
Detlef Günther	CERT-VW, Volkswagen AG
Jens Nedon	ConSecur GmbH
Dirk Schadt	SPOT Consulting

General Chair

Dirk Schadt — SPOT Consulting
dirk.schadt@spot.net

Program Chair

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

Sponsor Chair

Dirk Schadt — SPOT Consulting
dirk.schadt@spot.net

IMF 2008

4th International GI SIG SIDAR Conference on
IT Incident Management & IT Forensics

Mannheim, Germany
September 23 - 25, 2008

www.imf-conference.org
mailto:imf2008@gi-fg-sidar.de

SIDAR

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

German Informatics Society

September 23, 2008

Time	Presentation	Speaker
10:00	Registration	
10:30	Greeting and Introduction	
10:45	Key Note: Investigations and Prosecution in cases of Computer Crime – Overview of the National and International situation	Fred-Mario Silberbach, Federal Criminal Police Office (BKA)
11:30	A Forensic Computing Framework to fit any Legal System	Steven W. Wood, ALSTE Technologies GmbH, Germany
12:15	Using Observations of Invariant Behavior to Detect Malicious Agency in Distributed Environments	Thomas Richard McEvoy and Stephen Wolthusen Royal Holloway, University of London, UK
13:00	Lunch	
14:00	File Type Analysis Using Signal Processing Techniques and Machine Learning vs. file Unix Utility for Forensic Analysis	Serguei Mokhov, Concordia University Montreal, Canada
14:45	IPv6 Attacking Test Using ICMPv6 Messages + 6Foren: Online Forensics in IPv6 Network Environment	Liu Wu, Network Research Center of Tsinghua University, Beijing, P.R. China
15:30	Break	
16:00	Live Forensic Acquisition as Alternative to Traditional Forensic Processes	Marthie Lessing, Council for Scientific and Industrial Research, SA
16:45	Key Note: Network Infrastructure Forensics	Felix Lindner, Recurity Labs GmbH, Germany
17:30	FG-SIDAR meeting	
19:00	Social event	

September 24, 2008

Time	Presentation	Speaker
10:00	Greeting and Introduction	
10:15	Key Note: New Challenges for IT-Security Research in ICT	Udo Helmbrecht, President of Federal Office for Information Security (BSI)
11:00	Panel discussion: Challenges and interest conflicts in forensic investigations	Udo Helmbrecht, Klaus Brunnstein, Felix Freiling, Henrik Becker Moderation: Dirk Schadt
11:45	Reconstructing People's Lives: A Case Study in Teaching Forensic Computing	Felix Freiling, Thorsten Holz and Martin Mink University of Mannheim, Germany
12:30	Lunch	
13:30	Network Forensics of Partial SSL/TLS Encrypted Traffic Classification Using Clustering Algorithms	Meng-Da Wu and Stephen D. Wolthusen Royal Holloway, University of London, UK
14:15	Building a state tracing Linux Kernel	Chakravarthy Gundabattula and Vinay Vaiday, Symbiosis Deemed University, Pune, India
15:00	Break	
15:30	Formally Specifying Operational Semantics and Language Constructs of Forensic Lucid	Serguei Mokhov, Concordia University Montreal, Canada
16:00	Rump Session	Moderation: Felix Freiling, University of Mannheim, Germany
17:00	Conclusion	
17:15	End of day 2	

September 25, 2008 - Workshop Day

Time	Presentation	Speaker
09:15	Greeting and Introduction	
09:30	Leveraging EnCase for the Enterprise and Memory Analysis	Steven W. Wood, ALSTE Technologies GmbH, Germany
11:00	Break	
11:30	IT-Security, System- and Personnel Data Protection Auditing in a governmental sector	Volker Kozok, Federal Ministry of Defense, Germany
13:00	Lunch	
14:00	Best Practices - Internet Auditing	Andreas Rohr, Federal Ministry of Defense
14:45	Incident Management - Legal Aspects	Volker Kozok, Federal Ministry of Defense
15:30	Incident Management – Rechtliche Aspekte	Volker Kozok, Bundesministerium für Verteidigung
16:15	IT-Forensik	Frank Gärtner, Streitkräfteamt
17:00	End	
17:15	End of day 3	

In Cooperation with

SPOT Consulting

ConSecur security & consulting

IEEE COMPUTER SOCIETY

IAO Fraunhofer Institut Arbeitswirtschaft und Organisation

IEEE

RUS CERT