# 2018 11th International Conference on IT Security Incident Management & IT Forensics (IMF 2018)

**Hamburg, Germany**
**7-9 May 2018**

IEEE

**IEEE Catalog Number:** CFP1817I-POD
**ISBN:** 978-1-5386-6633-3

| | |
|---|---|
| IEEE Catalog Number: | CFP1817I-POD |
| ISBN (Print-On-Demand): | 978-1-5386-6633-3 |
| ISBN (Online): | 978-1-5386-6632-6 |

**Additional Copies of This Publication Are Available From:**

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

# 2018 11th International Conference on IT Security Incident Management & IT Forensics

# IMF 2018

## Table of Contents

**Preface** vii
**Conference Organization** viii
**Acknowledgements** x

## IMF 2018 Papers

On the Robustness of Random Walk Algorithms for the Detection of Unstructured P2P Botnets 3
*Dominik Muhs (Technische Universität Dresden), Steffen Haas (Universität Hamburg), Thorsten Strufe (Technische Universität Dresden), and Mathias Fischer (Universität Hamburg)*

Exploring the Processing of Personal Data in Modern Vehicles - A Proposal of a Testbed for Explorative Research to Achieve Transparency for Privacy and Security 15
*Alexandra Koch (Otto-von-Guericke University of Magdeburg), Robert Altschaffel (Otto-von-Guericke University of Magdeburg), Stefan Kiltz (Otto-von-Guericke University of Magdeburg), Mario Hildebrandt (Otto-von-Guericke University of Magdeburg), and Jana Dittmann (Otto-von-Guericke University of Magdeburg)*

Linux Memory Forensics: Expanding Rekall for Userland Investigation 27
*Johannes Stadlinger (Friedrich-Alexander University Erlangen-Nürnberg), Andreas Dewald (ERNW Research GmbH, Friedrich-Alexander University Erlangen-Nürnberg), and Frank Block (ERNW GmbH, Friedrich-Alexander University Erlangen-Nürnberg)*

mrsh-mem: Approximate Matching on Raw Memory Dumps 47
*Lorenz Liebler (University of Applied Sciences Darmstadt, Germany) and Frank Breitinger (University of New Haven, USA)*

Principles of Secure Logging for Safekeeping Digital Evidence 65
*Felix Freiling (Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)) and Edita Bajramovic (Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) / Framatome GmbH)*

Defeating the Secrets of OTP Apps 76
*Philip Polleit (Friedrich-Alexander-Universität Erlangen-Nürnberg) and Michael Spreitzenbarth (Friedrich-Alexander-Universität Erlangen-Nürnberg)*

Introducing Anti-Forensics to SQLite Corpora and Tool Testing 89
*Sven Schmitt (Friedrich-Alexander-University Erlangen-Nuremberg (FAU), Germany)*

Complexities in Investigating Cases of Social Engineering: How Reverse Engineering and Profiling can Assist in the Collection of Evidence 107
*Christina Lekati (Cyber Risk GmbH)*

Swimming in the Monero pools 110
*Emilien Le Jamtel (CERT-EU)*

The -Time-to-Compromise Metric for Practical Cyber Security Risk Estimation 115
*Andrej Zieger (HAW Hamburg), Felix Freiling (FAU Erlangen-Nürnberg), and Klaus-Peter Kossakowski (HAW Hamburg)*

**Author Index 135**