

2012 7th International Conference on Risks and Security of Internet and Systems

(CRiSIS 2012)

**Cork, Ireland
10 – 12 October 2012**



**IEEE Catalog Number: CFP1261F-PRT
ISBN: 978-1-4673-3087-9**

TABLE OF CONTENTS

| | |
|---|-----|
| Trust-based Delegation for Ad Hoc QoS Enhancing | 1 |
| <i>R. Abassi, S. Fatmi</i> | |
| A Vector Based Model Approach for Defining Trust in Multi-Organization Environments | 8 |
| <i>K. Toumi, C. Andres, A. Cavalli, M. Maarabani</i> | |
| Towards Efficient Access Control In A Mobile Agent Based Wireless Sensor Network | 16 |
| <i>E. Mercadal, G. Navarro-Arribas, S. Foley, J. Borrell</i> | |
| Privacy-by-Design Based on Quantitative Threat Modeling | 20 |
| <i>J. Luna, N. Suri, I. Krontiris</i> | |
| Modeling the Stuxnet Attack with BDMP: Towards More Formal Risk Assessments | 28 |
| <i>S. Kriaa, M. Bouissou, L. Pietre-Cambacedes</i> | |
| Detecting Attacks against Data in Web Applications | 36 |
| <i>R. Ludinard, E. Totel, F. Tronel, V. Nicomette, M. Kaaniche, E. Alata, R. Akrou, Y. Bachy</i> | |
| Partitioning the Internet | 44 |
| <i>M. Wachs, C. Grothoff, R. Thurimella</i> | |
| Improving the detection of On-line Vertical Port Scan in IP Traffic | 52 |
| <i>Y. Chabchoub, C. Fricker, P. Robert</i> | |
| Hash Pile Ups: Using Collisions to Identify Unknown Hash Functions | 58 |
| <i>R. Tobin, D. Malone</i> | |
| Investigating the Dark Cyberspace: Profiling, Threat-Based Analysis and Correlation | 64 |
| <i>C. Fachkha, E. Bou-Harb, A. Boukhtouta, S. Dinh, F. Iqbal, M. Debbabi</i> | |
| A Honeypot for Arbitrary Malware on USB Storage Devices | 72 |
| <i>S. Poeplau, J. Gassen</i> | |
| Evasion-Resistant Malware Signature Based on Profiling Kernel Data Structure Objects | 80 |
| <i>A. Shosha, C. Liu, P. Gladyshev, M. Matten</i> | |
| Browser Function Calls Modeling For Banking Malware Detection | 88 |
| <i>M. Garcia-Cervigon, M. Llinas</i> | |
| Don't Work. Can't Work? Why It's Time to Rethink Security Warnings | 95 |
| <i>K. Krol, M. Moroz, M. Sasse</i> | |
| Distributed e-Voting using the Smart Card Web Server | 103 |
| <i>L. Kyrillidis, S. Cobourne, K. Mayes, S. Dong, K. Markantonakis</i> | |
| Anomaly Analysis for Physical Access Control Security Configuration | 111 |
| <i>W. Fitzgerald, F. Turkmen, S. Foley, B. O'Sullivan</i> | |
| Security-Related Vulnerability Life Cycle Analysis | 119 |
| <i>G. Marconato, V. Nicomette, M. Kaaniche</i> | |
| Semantic Matching Of Web Services Security Policies | 127 |
| <i>M. Brahim, T. Chaari, M. Jemaa, M. Jmaiel</i> | |
| Managing and Accessing Data in the Cloud: Privacy Risks and Approaches | 135 |
| <i>S. Vimercati, S. Foresti, P. Samarati</i> | |
| CRiSIS 2012 Security Standards Tutorial | 144 |
| <i>S. Farrell</i> | |
| Semiring-based Constraint Models and Frameworks for Security-related Scenarios | 148 |
| <i>S. Bistarelli, F. Santini</i> | |
| Attacks Against Smart Cards: Hands On Session | 152 |
| <i>J. Lanet</i> | |
| Author Index | |