

Contents

System Security

| | |
|--|----|
| Event-Triggered Watermarking Control to Handle Cyber-Physical Integrity Attacks | 3 |
| <i>Jose Rubio-Hernan, Luca De Cicco, and Joaquin Garcia-Alfaro</i> | |
| Detecting Process-Aware Attacks in Sequential Control Systems. | 20 |
| <i>Oualid Koucham, Stéphane Mocanu, Guillaume Hiet, Jean-Marc Thiriet, and Frédéric Majorczyk</i> | |
| Towards an Automated and Dynamic Risk Management Response System. . . | 37 |
| <i>Gustavo Gonzalez-Granadillo, Ender Alvarez, Alexander Motzek, Matteo Merialdo, Joaquin Garcia-Alfaro, and Hervé Debar</i> | |
| Understanding How Components of Organisations Contribute to Attacks . . . | 54 |
| <i>Min Gu, Zaruhi Aslanyan, and Christian W. Probst</i> | |
| A Stochastic Framework for Prediction of Malware Spreading in Heterogeneous Networks | 67 |
| <i>Sandra König, Stefan Schauer, and Stefan Rass</i> | |

Network Security

| | |
|--|-----|
| Creating and Detecting IPv6 Transition Mechanism-Based Information Exfiltration Covert Channels. | 85 |
| <i>Bernhards Blumbergs, Mauno Pihelgas, Markus Kont, Olaf Maennel, and Risto Vaarandi</i> | |
| ML: DDoS Damage Control with MPLS | 101 |
| <i>Pierre-Edouard Fabre, Hervé Debar, Jouni Viinikka, and Gregory Blanc</i> | |

Software Security

| | |
|---|-----|
| Empirical Analysis on the Use of Dynamic Code Updates in Android and Its Security Implications. | 119 |
| <i>Maqsood Ahmad, Bruno Crispo, and Teklay Gebremichael</i> | |
| Evaluation of Resource-Based App Repackaging Detection in Android | 135 |
| <i>Olga Gadyatskaya, Andra-Lidia Lezza, and Yuri Zhauniarovich</i> | |

A Survey on Internal Interfaces Used by Exploits and Implications on
Interface Diversification 152
*Sampsa Rauti, Samuel Lauren, Joni Uitto, Shohreh Hosseinzadeh,
Jukka Ruohonen, Sami Hyrynsalmi, and Ville Leppänen*

A Tale of the OpenSSL State Machine: A Large-Scale Black-Box Analysis . . . 169
Joeri de Ruiter

Cryptography

Speeding up R-LWE Post-quantum Key Exchange 187
Shay Gueron and Fabian Schlieker

Efficient Sparse Merkle Trees: Caching Strategies and Secure (Non-)
Membership Proofs 199
Rasmus Dahlberg, Tobias Pulls, and Roel Peeters

Secure Multiparty Sorting Protocols with Covert Privacy 216
Peeter Laud and Martin Pettai

Authentication

PASSPHONE: Outsourcing Phone-Based Web Authentication While
Protecting User Privacy 235
Martin Potthast, Christian Forler, Eik List, and Stefan Lucks

Secure, Usable and Privacy-Friendly User Authentication from Keystroke
Dynamics. 256
Kimmo Halunen and Visa Vallivaara

Author Index 269

Secure IT Systems

21st Nordic Conference, NordSec 2016, Oulu, Finland,

November 2-4, 2016. Proceedings

Brumley, B.B.; Röning, J. (Eds.)

2016, X, 269 p. 43 illus., Softcover

ISBN: 978-3-319-47559-2