Contents

Cryptographic Protocols

Coercion-Resistant Proxy Voting .................................................. 3
   Oksana Kulyk, Stephan Neumann, Karola Marky, Jurlind Budurushi,
   and Melanie Volkamer

A Posteriori Openable Public Key Encryption ................................ 17
   Xavier Bultel and Pascal Lafourcade

Multicast Delayed Authentication for Streaming Synchrophasor Data
   in the Smart Grid ................................................................. 32
   Sérgio Câmara, Dhananjay Anand, Victoria Pillitteri, and Luiz Carmo

Human Aspects of Security

Developing a Human Activity Model for Insider IS Security Breaches
   Using Action Design Research .............................................. 49
   Gurpreet Dhillon, Spyridon Samonas, and Ugo Etudo

Evaluating CVSS Base Score Using Vulnerability Rewards Programs .... 62
   Awad Younis, Yashwant K. Malaiya, and Indrajit Ray

Defining Objectives for Preventing Cyberstalking ........................... 76
   Gurpreet Dhillon, Chandrashekar Challa, and Kane Smith

Cyber Infrastructure

Using Process Invariants to Detect Cyber Attacks on a Water
   Treatment System ............................................................... 91
   Sridhar Adepu and Aditya Mathur

Expression and Enforcement of Security Policy for Virtual Resource
   Allocation in IaaS Cloud ...................................................... 105
   Yanhuang Li, Nora Cuppens-Boulahia, Jean-Michel Crom,
   Frédéric Cuppens, and Vincent Frey

Software Defined Networking Reactive Stateful Firewall .................. 119
   Salaheddine Zerkane, David Espes, Philippe Le Parc,
   and Frederic Cuppens
Phishing and Data Sharing

Teaching Phishing-Security: Which Way is Best? .............................. 135
  Simon Stockhardt, Benjamin Reinheimer, Melanie Volkamer,
  Peter Mayer, Alexandra Kunz, Philipp Rack, and Daniel Lehmann

On Gender Specific Perception of Data Sharing in Japan .................. 150
  Markus Tschersich, Shinsaku Kiyomoto, Sebastian Pape,
  Toru Nakamura, Gökhan Bal, Haruo Takasaki, and Kai Rannenberg

TORPEDO: TOoltip-poweRed Phishing Email DetectiOn ...................... 161
  Melanie Volkamer, Karen Renaud, and Benjamin Reinheimer

Social Networks

SybilRadar: A Graph-Structure Based Framework for Sybil Detection
in On-line Social Networks ......................................................... 179
  Dieudonné Mulamba, Indrajit Ray, and Indrakshi Ray

Collateral Damage of Facebook Apps: Friends, Providers,
and Privacy Interdependence ...................................................... 194
  Iraklis Symeonidis, Fatemeh Shirazi, Gergely Biczók,
  Cristina Pérez-Solà, and Bart Preneel

Software Vulnerabilities

Automated Source Code Instrumentation for Verifying Potential
Vulnerabilities ................................................................. 211
  Hongzhe Li, Jaesang Oh, Hakjoo Oh, and Heejo Lee

An Information Flow-Based Taxonomy to Understand the Nature
of Software Vulnerabilities ..................................................... 227
  Daniela Oliveira, Jedidiah Crandall, Harry Kalodner, Nicole Morin,
  Megan Maher, Jesus Navarro, and Felix Emiliano

XSS PEEKER: Dissecting the XSS Exploitation Techniques and Fuzzing
Mechanisms of Blackbox Web Application Scanners ....................... 243
  Enrico Bazzoli, Claudio Criscione, Federico Maggi, and Stefano Zanero

TPM and Internet of Things

A Utility-Based Reputation Model for the Internet of Things .............. 261
  Benjamin Aziz, Paul Fremantle, Rui Wei, and Alvaro Arenas

Advanced Remote Firmware Upgrades Using TPM 2.0 ..................... 276
  Andreas Fuchs, Christoph Krauß, and Jürgen Repp
Sidechannel Analysis

RegRSA: Using Registers as Buffers to Resist Memory Disclosure Attacks. . . 293
  Yuan Zhao, Jingqiang Lin, Wuqiong Pan, Cong Xue, Fangyu Zheng,
  and Ziqiang Ma

Uncertain? No, It’s Very Certain!: Recovering the Key from Guessing
Entropy Enhanced CPA ................................................................. 308
  Changhai Ou, Zhu Wang, Degang Sun, Xinpeng Zhou, and Juan Ai

Software Security

Advanced or Not? A Comparative Study of the Use of Anti-debugging
and Anti-VM Techniques in Generic and Targeted Malware....................... 323
  Ping Chen, Christophe Huygens, Lieven Desmet, and Wouter Joosen

NativeProtector: Protecting Android Applications by Isolating
and Intercepting Third-Party Native Libraries ........................................ 337
  Yu-Yang Hong, Yu-Ping Wang, and Jie Yin

A Progress-Sensitive Flow-Sensitive Inlined Information-Flow
Control Monitor .................................................................................... 352
  Andrew Bedford, Stephen Chong, Josée Desharnais, and Nadia Tawbi

Privacy

Deducing User Presence from Inter-Message Intervals in Home
Automation Systems .................................................................................. 369
  Frederik Möllers and Christoph Sorge

Privacy by Design Principles in Design of New Generation Cognitive
Assistive Technologies. ........................................................................... 384
  Ella Kolkowska and Annica Kristofferson

A Trustless Privacy-Preserving Reputation System ................................. 398
  Alexander Schaub, Rémi Bazin, Omar Hasan, and Lionel Brunie

Author Index ......................................................................................... 413
ICT Systems Security and Privacy Protection
31st IFIP TC 11 International Conference, SEC 2016,
Ghent, Belgium, May 30 - June 1, 2016, Proceedings
Hoepman, J.-H.; Katzenbeisser, S. (Eds.)
2016, XIII, 414 p. 82 illus., Hardcover
ISBN: 978-3-319-33629-9