Table of Contents

Preface .................................................................................................................................................... xvi

Section 1
Secure Software Development Process

Chapter 1
Agile Software Development: The Straight and Narrow Path to Secure Software? ......................... 1
Torstein Nicolaysen, NTNU, Norway
Richard Sassoon, NTNU, Norway
Maria B. Line, SINTEF ICT, Norway
Martin Gilje Jaatun, SINTEF ICT, Norway

Chapter 2
Assimilating and Optimizing Software Assurance in the SDLC: A Framework and Step-Wise Approach ........................................................................................................................................... 16
Aderemi O. Adeniji, University of North Carolina at Charlotte, USA
Seok-Won Lee, University of North Carolina at Charlotte, USA

Chapter 3
Towards Designing E-Services that Protect Privacy .............................................................................. 35
George O. M. Yee, Carleton University, Canada

Section 2
Security Requirements Analysis and Modeling

Chapter 4
Software Engineering Security Based on Business Process Modeling ............................................. 52
Joseph Barjis, Delft University of Technology, The Netherlands
Chapter 5
Integrating Access Control into UML for Secure Software Modeling and Analysis

Thuong Doan, University of Connecticut, USA
Steven Demurjian, University of Connecticut, USA
Laurent Michel, University of Connecticut, USA
Solomon Berhe, University of Connecticut, USA

Chapter 6
Benefits and Challenges in the Use of Case Studies for Security Requirements Engineering Methods

Nancy R. Mead, Carnegie Mellon University, USA

Chapter 7
Security Requirements Engineering for Evolving Software Systems: A Survey

Armstrong Nhlabatsi, The Open University, UK
Bashar Nuseibeh, Lero, Ireland & The Open University, UK
Yijun Yu, The Open University, UK

Section 3
Vulnerability Detection

Chapter 8
Monitoring Buffer Overflow Attacks: A Perennial Task

Hossain Shahriar, Queen’s University, Canada
Mohammad Zulkernine, Queen’s University, Canada

Chapter 9
CONFU: Configuration Fuzzing Testing Framework for Software Vulnerability Detection

Huning Dai, Columbia University, USA
Christian Murphy, Columbia University, USA
Gail Kaiser, Columbia University, USA

Section 4
Protection Mechanisms

Chapter 10
Retrofitting Existing Web Applications with Effective Dynamic Protection Against SQL Injection Attacks

San-Tsai Sun, University of British Columbia, Canada
Konstantin Beznosov, University of British Columbia, Canada
Chapter 11
Improving Memory Management Security for C and C++ ............................. 190
Yves Younan, Katholieke Universiteit Leuven, Belgium
Wouter Joosen, Katholieke Universiteit Leuven, Belgium
Frank Piessens, Katholieke Universiteit Leuven, Belgium
Hans Van den Eynden, Katholieke Universiteit Leuven, Belgium

Chapter 12
Katana: Towards Patching as a Runtime Part of the Compiler-Linker-Loader Toolchain ........ 217
Sergey Bratus, Dartmouth College, USA
James Oakley, Dartmouth College, USA
Ashwin Ramaswamy, Dartmouth College, USA
Sean W. Smith, Dartmouth College, USA
Michael E. Locasto, George Mason University, USA

Chapter 13
A Formal Approach for Securing XML Document ................................................ 234
Yun Bai, University of Western Sydney, Australia

Chapter 14
A Tool Support for Secure Software Integration .................................................. 248
Khaled M. Khan, Qatar University, Qatar
Jun Han, Swinburne University of Technology, Australia

Chapter 15
Towards Tool-Support for Usable Secure Requirements Engineering with CAIRIS .............. 269
Shamal Faily, University of Oxford, UK
Ivan Fléchais, University of Oxford, UK

Chapter 16
Secure Software Education: A Contextual Model-Based Approach .......................... 286
J. J. Simpson, System Concepts, LLC, USA
M. J. Simpson, System Concepts, LLC, USA
B. Endicott-Popovsky, University of Washington, USA
V. Popovsky, University of Idaho, USA
Chapter 17
Development of a Master of Software Assurance Reference Curriculum ........................................ 313
   Nancy R. Mead, Carnegie Mellon University, USA
   Julia H. Allen, Carnegie Mellon University, USA
   Mark Ardis, Stevens Institute of Technology, USA
   Thomas B. Hilburn, Embry-Riddle Aeronautical University, USA
   Andrew J. Kornecki, Embry-Riddle Aeronautical University, USA
   Rick Linger, Carnegie Mellon University, USA
   James McDonald, Monmouth University, USA

Chapter 18
A Rigorous Approach to the Definition of an International Vocational Master’s Degree in Information
Security Management ........................................................................................................................ 328
   Frédéric Girard, Henri Tudor Public Research Center, Luxembourg
   Bertrand Meunier, Henri Tudor Public Research Center, Luxembourg
   Duan Hua, Henri Tudor Public Research Center, Luxembourg
   Eric Dubois, Henri Tudor Public Research Center, Luxembourg

Compilation of References ............................................................................................................ 344

About the Contributors .................................................................................................................... 375

Index ................................................................................................................................................... 386