Software Security Engineering: Design and Applications

Reviewed by Khaled M. Khan, Qatar University, Qatar

Muthu Ramachandran from Leeds Metropolitan University, UK has recently published a book entitled, *Software Security Engineering: Design and Applications*. The author claims that the book provides systematic approaches to engineering, building and assuring software security throughout software lifecycle, software security based requirements engineering, design for software security, software security implementation, best practice guideline on developing software security, test for software security, and quality validation for software security. The book uses UML 2.0 for modelling and design examples. A running case study called Qbay (Quality-Bay auction system) has been used throughout the book in all chapters. It also provides some insights into software requirements engineering for security, current issues in software security, and to show how to build secure applications with appropriate selection of principles and process. Its aim is to provide concise and good practice design guidelines on software security which are expected to benefit practitioners, researchers, learners, and educators. This book provides software security best practices that practitioners and researchers can use in their everyday life. This book has been divided into three parts.

Part 1 dedicates to Software Security Requirements Engineering & Management in order to provide overview of techniques and methods on software security requirements engineering, software security modelling, interrelated concepts of knowledge engineering, software security engineering with software product line engineering which is unique approach supporting SPL, software security assurance and its management aspects including how social engineering concepts can be used to elicit software security requirements. This part also provides a comprehensive guide to SSE process, taxonomies, threat analysis using Microsoft SDL tool.

Part 2 discusses topics such as design for security, component based design for software security, best practice development guidelines,
software security testing, and an improvement model for security practices. One of the unique contributions of this is on design for software security which provides security specialists and software engineers to consider design techniques to build software security in from requirements. The chapter on software security testing provides techniques, guidelines, and detailed documentation templates for various test strategies that can be adopted systematically.

Part 3 concentrates on two important applications such as cloud computing and Enterprise Wide Resource Planning (ERP). This section provides very interesting applications that are in high demand. The cloud computing application looks at how to design cloud services with software security built-in using software components. This method has been illustrated with Amazon EC2 cloud architecture.

In summary, this book claims to provide concise and good practice design guidelines on software security which are expected to benefit practitioners, researchers, learners, and educators. Topics discussed include building and assuring software security throughout software lifecycle; software security based requirements engineering; software security implementation; best practice guideline on developing software security; test for software security and quality validation for software security. Nova Scientific Publishers has published this book in 2011.

Khaled M. Khan is serving the Department of Computer Science and Engineering at Qatar University. He also holds an honorary adjunct fellow position in the School of Computing and Mathematics at the University of Western Sydney (Australia). Prior to these positions, Dr. Khan served as an academic in computing at the University of Western Sydney for seven years. He was the head of programs for the postgraduate computing courses at the University of Western Sydney for six years. He has taught computing last twenty years at various universities in Asia, Europe, Africa and Australia. His research interests include software security, software component, software architecture, Web services and service-oriented software. He received his PhD in computing from Monash University and a BS and MS in computer science and informatics from the Norwegian University of Science and Technology (Norway). He also holds a second bachelor's degree from the University of Dhaka (Bangladesh). Dr. Khan has published more than fifty refereed papers and additionally has edited two books. Dr. Khan is currently serving several editorial boards of different journals and conference program committees. He contributed to the IEEE-ACM Computing Curricula 2001.