Software Engineering for Secure Systems:
Industrial and Research Perspectives

Haralambos Mouratidis
University of East London, UK
### Detailed Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>xiii</td>
</tr>
<tr>
<td>Preface</td>
<td>xiv</td>
</tr>
<tr>
<td>Acknowledgment</td>
<td>xvii</td>
</tr>
</tbody>
</table>

#### Chapter 1
State of Practice in Secure Software: Experts’ Views on Best Ways Ahead

  * Bill Whyte, Independent Consultant, UK
  * John Harrison, LanditD, UK

In this chapter the authors present a synthesis of expert views on some important actions to improve the state of practice in secure software. The authors base their study on experiences as panel moderators, rapporteurs and report writers involved in drafting the views of experts.

**Section 1**

**Security Patterns**

#### Chapter 2
Using Security Patterns to Develop Secure Systems

  * Eduardo B. Fernandez, Florida Atlantic University, USA
  * Nobukazu Yoshioka, GRACE Center, National Institute of Informatics, Japan
  * Hironori Washizaki, Waseda University, Japan
  * Jan Jurjens, Technical University of Dortmund, Germany
  * Michael VanHilst, Florida Atlantic University, USA
  * Guenther Pernu, University of Regensburg, Germany

In this chapter the authors present work on the use of patterns for the development of secure software systems. Their work applies the pattern paradigm to various parts of the software systems development from analysis to design to testing.
Chapter 3
A Pattern-Based Method to Develop Secure Software

Holger Schmidt, Technical University Dortmund, Germany
Denis Hatebur, University Duisburg-Essen and ITESYS Institut für Technische
Systeme GmbH, Germany
Maritta Heisel, University Duisburg-Essen, Germany

In this chapter, the authors discuss a security engineering process based on security problem frames and concretized security problem frames. The presented process is supported by formal models that are used to prove that the solution approaches are correct solutions to the security problems. Furthermore, the formal models of the solution approaches constitute a formal specification of the software to be developed.

Chapter 4
Security Patterns: Comparing Modeling Approaches

Armstrong Nhlabatsi, The Open University, UK
Arosha Bandara, The Open University, UK
Shinpei Hayashi, Tokyo Institute of Technology, Japan
Charles B. Haley, The Open University, UK
Jan Jurjens, The Open University, UK
Haruhiko Kaiya, Shinshu University, Japan
Atsuto Kubo, National Institute of Informatics, Japan
Robin Laney, The Open University, UK
Haralambos Mouratidis, University of East London, UK
Thein T. Tun, The Open University, UK
Hironori Washizaki, Waseda University, Japan
Nobukazu Yoshioka, National Institute of Informatics, Japan
Yijun Yu, The Open University, UK

The authors of this chapter present evaluation results of a study that examined the extent to which constructs provided by security requirements engineering approaches can support the use of security patterns as part of the analysis of security problems. Their analysis was based on a specific pattern and it employ a number of existing security modelling approaches.
Section 2
Methodologies and Frameworks

Chapter 5
Security Over the Information Systems Development Cycle .................................................. 113
C. Blanco, University of Cantabria, Spain
D. G. Rosado, University of Castilla-La Mancha, Spain
C. Gutiérrez, Correos Telecom, Spain
A. Rodríguez, University of Bio-Bio, Chile
D. Mellado, Spanish Tax Agency, Madrid, Spain
E. Fernández-Medina, University of Castilla-La Mancha, Spain
J. Trujillo, University of Alicante, Spain
M. Piattini, University of Castilla-La Mancha, Spain

In this chapter the authors discuss the problem of integrating security into the software development process, paying more attention to the requirements engineering discipline and the software design stage, and they present their efforts to integrate security considerations into the software systems development process in various domains such as software product lines, business processes, web services, and databases and data warehouses.

Chapter 6
Balancing Security and Performance Properties During System Architectural Design ........ 155
Siv Hilde Houmb, Telenor GBDR Platform for Service Innovation Group, Norway
Geri Georg, Colorado State University, USA
Dorina C. Petriu, Carleton University, Canada
Behzad Bordbar, University of Birmingham, UK
Indrakshi Ray, Colorado State University, USA
Kyriakos Anastasakis, University of Birmingham, UK
Robert B. France, Colorado State University, USA

The authors present the Aspect-Oriented Risk Driven Development (AORDD) methodology, which integrates the analysis of two quality properties, namely security and performance, into the development process of critical systems. The approach is illustrated using a transactional web e-commerce benchmark (TPC-W) originally developed by the Transaction Processing Performance Council.

Chapter 7
State Model Diagrams: A Universal, Model Driven Method for Network System Configuration and Management ................................................................. 192
S. P. Maj, Edith Cowan University, Australia

This chapter presents an approach concerned with the configuration and management of network devices. In particular, the paper demonstrates how the State Model Diagram method is useful for the configuration and management of complex security protocols and devices.
Section 3
Privacy and Trust

Chapter 8
Designing Privacy Aware Information Systems .......................................................... 212
Christos Kalloniatis, University of the Aegean, Greece
Evangelia Kavaki, University of the Aegean, Greece
Stefanos Gritzalis, University of the Aegean, Greece

In this chapter the authors identify a number of privacy requirements that should be considered during system analysis and design. They also present and analyse 10 methods from the area of secure requirements engineering. They then compare these methods based on their initial set of privacy requirements.

Chapter 9
Privacy Aware Systems: From Models to Patterns ..................................................... 232
Alberto Coen-Porisini, Università degli studi dell’Insubria, Italy
Pietro Colombo, Università degli studi dell’Insubria, Italy
Sabrina Sicari, Università degli studi dell’Insubria, Italy

In this chapter, the authors present their work on the development of a conceptual model to support the definition of privacy policies. The presented model introduces a set of concepts concerning privacy and defines the existent relationships among those concepts along with the interfaces for the definition of privacy related mechanisms. The assessment of the model is presented with the aid of an example from the health domain.

Chapter 10
Incorporating Social Trust into Design Practices for Secure Systems ....................... 260
Piotr Cofia, BT (British Telecom), UK
Hazel Lacohée, BT (British Telecom), UK
Paul Hodgson, BT (British Telecom), UK

In this chapter, the authors discuss how the “designing for trust” paradigm leverages trust governance into the design practices of ICT systems by complementing security-based methodologies. In particular, they argue about the need to consider trust as part of the software systems development process, they present three different (but complimenting) views of the notion of trust and they discuss how trust governance and security management can benefit from an integration.
Section 4
Secure Code Analysis

Chapter 11
Static Program Analysis of Multi-Applet Java Card Applications ........................................... 286
Alexandros Loizidis, Aristotle University of Thessaloniki, Greece
Vasilios Almaliotis, Aristotle University of Thessaloniki, Greece
Panagiotis Katsaros, Aristotle University of Thessaloniki, Greece

In this chapter the authors investigate recent advances in theory and tool support for static program analysis of security critical applications. Based on their investigation they then present an approach for automatic verification of critical application based on the domain of smart cards.

Chapter 12
Automatic Timed Automata Extraction from Ladder Programs for Model-Based Analysis of Control Systems ................................................................. 305
Kêzia de Vasconcelos Oliveira, Federal University of Campina Grande, Brazil
Kyller Gorgônio, Federal University of Campina Grande, Brazil
Angelo Perkusich, Federal University of Campina Grande, Brazil
Antônio Marcus Nogueira Lima, Federal University of Campina Grande, Brazil
Leandro Dias da Silva, Federal University of Alagoas, Brazil

In this chapter the authors present a method to increase the confidence in the behavior of critical control systems. The presented method automatically generates the timed automata models from the specification ISA 5.2 Binary Logic Diagrams, and the implementation Ladder programs, for model-based analysis. The method is based on the use of the Uppaal tool and the Uppaal-TRON testing tool.

Compilation of References ................................................................. 329
About the Contributors ................................................................. 353
Index ......................................................................................... 366