

Preface

This book presents the results of research related to the development and dynamic deployment and adjustment of solutions that enhance the security and dependability of Ambient Intelligence (AmI) ecosystems, i.e. dynamic, open environments characterised by the coexistence of distributed and highly heterogeneous applications, devices, and users that interact and collaborate in order to achieve their goals. The book is based on research that has been undertaken as part of the SERENITY project, an integrated project funded by the European Framework 6 Programme, which started in January 2006 and ended in December 2008.

The general aim of SERENITY has been to enhance security and dependability of AmI ecosystems by providing a framework supporting the development, integration, configuration, monitoring and adaptation of security and dependability mechanisms for such systems. The key approach in the development of this framework is the use of *security and dependability (S&D) patterns*. The purpose of these patterns is to encode the knowledge and experience of experts in security and dependability mechanisms into models that describe the mechanisms and their deployment, and make them available to application developers for use.

The approach undertaken in SERENITY builds upon earlier experience in the use of patterns for modeling security and dependability solutions. However, it models and uses patterns in novel ways, most notably to support the automatic selection, deployment, integration, monitoring and adaptation of S&D solutions at runtime. The S&D patterns of SERENITY advance previous work by modeling explicitly the security and dependability properties which are achieved by different solutions and contextual conditions for the successful deployment of these solutions that should be monitored at runtime. SERENITY S&D patterns provide also direct links to implementations that can be used to achieve dynamic invocation, integration and adaptation of solutions during the operation of AmI ecosystems. To realize its approach, SERENITY has developed advanced methods, tools, and techniques for the specification and formal verification of patterns, and runtime frameworks for (a) selecting, configuring linking and adapting S&D solutions for applications at runtime, and (b) detecting, diagnosing and reacting to violations or potential violations (threats) of conditions that underpin the deployment of these solutions at runtime. The operations of both these frameworks are driven by S&D patterns.

Research results of SERENITY have been published in various scientific fora during the course of the project. This book complements earlier publications by providing the first advanced and integrated account of the tools, methods and techniques that have been developed in the project and discussing them in the context of the broader related literature. To provide a succinct and non SERENITY-biased view over this literature, we have also included two chapters that cover the broader themes of security and dependability engineering and the use of security and dependability patterns in system engineering. These chapters

have been written by internationally renowned researchers outside the SERENITY consortium.

Following an introductory chapter providing an overview of the problem of security and dependability in AmI ecosystems and the SERENITY approach to this problem, this book is organized in six parts. Part A covers the foundations of security and dependability engineering. Part B gives an account of the representation of security and dependability solutions in SERENITY based on the notion of S&D Patterns and provides examples of such patterns for different types of systems and technologies. Part C discusses the processes for developing security and dependability solutions in SERENITY and applications that can make use of these solutions through the support of the SERENITY framework. Part D discusses the runtime framework of SERENITY and the support that it offers for the dynamic selection, configuration, monitoring and adaptation of S&D solutions as part of different applications. Part E includes chapters which consider the problem of security and dependability from organizational and legal perspectives and cover work that has been undertaken in SERENITY in these areas. Finally, Part F provides a number of case studies demonstrating the use of the SERENITY approach and supporting technologies in different domains, and reporting relevant experiences. The final part of the book includes an overview of directions for further research for the enhancement of SERENITY.

Our hope is that this book will be useful to professionals and researchers with an interest in security and dependability engineering for highly distributed and dynamically adjustable AmI ecosystems. Our coverage of the subject has inevitably been biased by the “SERENITY approach” and, to this end, it might not cover related work to the extent that different individual readers would expect. We apologise for this hoping that readers will appreciate that a detailed coverage of all related approaches had not been our main objective during the preparation of the book. We also hope that, despite its partiality in this respect, the book will still be useful to researchers and practitioners and enjoyed.

Finally, we would like to warmly thank all the authors who have contributed to this book and the reviewers who provided indispensable and constructive advice for the selection and improvement of the chapters in it. Last but not least, we thank the European Commission for supporting financially the research of SERENITY (FP6-IST-2006-27587) and Springer for trusting us and supporting this publication.

December 2008

*George Spanoudakis
Antonio Maña
Spyros Kokolakis*

Security and Dependability for Ambient Intelligence

Spanoudakis, G.; Kokolakis, S. (Eds.)

2009, IX, 392 p. 80 illus., 30 illus. in color., Hardcover

ISBN: 978-0-387-88774-6