Security Patterns

Integrating Security and Systems Engineering

Markus Schumacher
Eduardo Fernandez-Buglioni
Duane Hybertson
Frank Buschmann
Peter Sommerlad

John Wiley & Sons, Ltd

Security Patterns

Security Patterns

Integrating Security and Systems Engineering

Markus Schumacher
Eduardo Fernandez-Buglioni
Duane Hybertson
Frank Buschmann
Peter Sommerlad

John Wiley & Sons, Ltd

John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester,
West Sussex PO19 8SQ, England
Telephone (+44) 1243 779777

Email (for orders and customer service enquiries): cs-books@wiley.co.uk
Visit our Home Page on www.wiley.com

Other Wiley Editorial Offices

John Wiley & Sons Inc., 111 River Street, Hoboken, NJ 07030, USA

Jossey-Bass, 989 Market Street, San Francisco, CA 94103-1741, USA

Wiley-VCH Verlag GmbH, Boschstr. 12, D-69469 Weinheim, Germany

John Wiley & Sons Australia Ltd, 42 McDougall Street, Milton, Queensland 4064, Australia

John Wiley & Sons (Asia) Pte Ltd, 2 Clementi Loop #02-01, Jin Xing Distripark, Singapore 129809

John Wiley & Sons Canada Ltd, 22 Worcester Road, Etobicoke, Ontario, Canada M9W 1L1

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Library of Congress Cataloging-in-Publication Data

Security patterns : integrating security and systems engineering / Markus Schumacher ... [et al.].
p. cm.
Includes bibliographical references and index.
ISBN-13: 978-0-470-85884-4 (cloth : alk. paper)
ISBN-10: 0-470-85884-2 (cloth : alk. paper)
1. Computer security. 2. Systems engineering. I. Schumacher, Markus.

QA76.9.A25S438 2005
005.8--dc22

2005026865

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN-13 978-0-470-85884-4 (HB)
ISBN-10 0-470-85884-2 (HB)

Typeset in 10/12pt Sabon by Laserwords Private Limited, Chennai, India
Printed and bound in Great Britain by Anthony Rowe Ltd, Chippenham, Wiltshire
This book is printed on acid-free paper responsibly manufactured from sustainable forestry
in which at least two trees are planted for each one used for paper production.

For you, dear reader!
Go and create secure software systems.

Markus

To Minjie, Lian, and Anna.

Eduardo

For my wife, Diane, for making considerable sacrifice to allow me to work on this book.

Duane

For Martina, Bebé, and Anna.

Frank

For Andrea.

Peter

Contents

Foreword

Security has become an important topic for many software systems. With the growing success of the Internet, computer and software systems have become more and more networked. Researchers are already developing scenarios in which millions of devices are connected and cooperatively running web-based commerce, government, health, and other types of security-sensitive systems. Much of the research effort in these scenarios is devoted to security aspects.

What could happen if, in a pervasive health scenario, cardiology data collected by wireless sensors attached to your body and pre-processed by software on your PDA is intercepted and manipulated by an unauthorized person during its transmission to your doctor? Or think of a scenario in which the software in your car is updated remotely because an attacker has compromised the manufacturer's servers. What if your car, which has just been 'updated,' no longer brakes, but instead activates its drive-by-wire accelerator? What if, in the near future, the control tower that just took over handling of the aircraft in which you are a passenger discovers that the plane no longer does what the pilots or the tower want, but, instead, what some hijackers want it to do? Perhaps worst of all, think about potential for disaster should someone maliciously take over control of a nuclear power plant…

You simply do not want these things to happen! In other words, you require the system to ensure a proper level of confidentiality and integrity before you trust and use it.

Although the importance of security is widely acknowledged, only a few projects address it with the appropriate priority. Security is still an afterthought in many projects. Check the latest security articles in your favorite IT magazine, and you will find reports of successful intrusions into, or denial of service attacks against, all sorts of enterprise-level systems—which, ironically enough, are often not performed by experts, but by high-school kids or students via very simple measures like scripts.

So why is there this discrepancy between the acknowledgement of security and its prioritization in software development? Certainly not because security is still an

unexplored field in software. Moreover, security requirements are often expressed vaguely or not at all, and software architectures often expose limited security-related decisions. To survive in today's networked and open computing world, it is crucial to go beyond the realms of authentication.

Project managers, software architects, developers, testers, and other stakeholders of a software system need to ensure that security is an integral part of all software projects.

This is where the book you are holding steps in. Unlike other books on the market that tend to cover the latest research ideas and new security technologies, this new book covers real-world knowledge and experience from international security experts. It uses patterns, a successful and widely adopted technology for describing, communicating, and sharing knowledge. The authors guide you through the field of security, address key questions, and clearly show you how to build secure systems, and present corresponding proven solutions.

For example, how do you identify an organization's or system's security needs, and how do you define an appropriate security approach to meet these needs? Is confidentiality a security property you need in your system, or integrity, availability, or accountability? Or even a mixture of the four? And how do you ensure these properties by appropriate means of prevention, detection, and response? Via identification and authentication (I&A)? Or do you also need a means of access control and authorization in your systems, or even accounting and auditing? And how do all services interact to provide a consistent and coherent security concept for your system? Once you know what security services you need and how they interoperate, what are their different realization options? For example, is a password-based or a PKI-based I&A appropriate to meet your security needs? And what different options are available to you? Smart cards? RFID tags? Or is it sufficient that you provide a log-on service for your system that requests your user ID and password?

You can imagine such a list of questions can be continued and detailed, not only for identification and authentication, but also for all other security services and mechanisms that can be provided: access control and authorization, accounting and auditing, and so on.

So while security is a wide and non-trivial field, it is nevertheless important that you address it appropriately in order to build successful software systems. Ignoring security due to lack of overview and knowledge could be catastrophic. I'm not a security expert, but after working on this book I had a much better understanding of the topic, allowing me to address it more explicitly, more prominently, and more constructively in my daily work as a software architect.

In addition to the technical value and contribution of this book, there is another aspect that makes it special. This book has been written from the heart of the patterns community. All its authors have carefully crafted the scope of their patterns to avoid overlap, and they have integrated all the relationships between the patterns to ensure a common look-and-feel. The result is a network of complementary, mutually-supporting patterns that provide a solid coverage of important security

areas. The value of this network is significantly bigger than the sum of the values of all its constituent patterns: you get the whole picture, not just its individual bits and pieces.

Finally, I'd like to invite you to take the opportunity to read and enjoy the patterns presented in this book. I hope that the security issues prove relevant for your systems, enrich your design knowledge, and enhance your overall understanding of security.

I'm sure you'll like this book as much as I do.

Frank Buschmann

Senior Principal Engineer
Siemens AG, Corporate Technology

About this Book

Much attention has recently been devoted to security issues, and it has become apparent that a high security level should be a fundamental prerequisite for all business processes—both in the commercial and public sector. The steadily increasing number of reported security incidents indicates that organizations need additional help in addressing basic security issues, ranging from enterprise plans through software systems to operational practices.

In general, security is not adequately addressed in enterprises and the systems that they build and operate. One reason is that security covers a broad area: it is a big challenge to define secure business processes and to develop and operate the corresponding systems and applications securely. The situation is becoming more challenging because of the increasing openness of systems and enterprises, due largely to the rise of the Internet and e-business technologies. It is very difficult achieve security, especially in distributed environments, as there are many different organizations, individuals, technical components and mechanisms involved. In addition, trust relationships change frequently, which makes a complete analysis of security requirements very hard. As modern business processes become more and more complex, the overall problem space is no longer easily comprehensible for the people involved. Specifically, there are three key issues:

- Security is often an afterthought in system design and implementation. The enterprise context and requirements that drive system security are not addressed explicitly, and are not incorporated into system architectures. What is needed is to begin to address security up-front, rather than the 'repair-service' approach we observe today.
- Many security breaches can be traced back to well-known security problems that still appear over and over again. Default passwords that are documented in the software manual are one example. Storing sensitive information on a public Web server is another example. These are manifestations that security is

being given a low priority, or of a lack of understanding of security issues. The dominant goal in these cases is to enhance functionality and performance, not to mitigate risk.

- Enterprise planners, system architects and developers, and operations managers have inadequate knowledge of security. As a consequence, they rely heavily on security specialists to understand their security needs and to provide security solutions. However, there are not enough security specialists to satisfy the need. Furthermore, in many cases, the security specialists find themselves repeating the same solutions for each enterprise or each system development project. This is an unnecessary waste of their time, and keeps them from addressing more complicated problems.

The key to addressing these issues is that—while many security problems are new or complicated—a significant number of basic security problems in an enterprise context are well understood, and well-established solutions exist for them. Over time, the security specialists who have encountered the same basic problems and found themselves repeating the same basic solutions have developed a good understanding of these problems and solutions. To some degree, these have been captured in the security literature and in security-related standards. But the knowledge codified in the literature and standards is not readily accessible to those who do not devote full time to security.

The purpose of this book is to capture some of these basic problems and solutions, and to make them available in a form usable by enterprise planners, system architects and developers, and operations managers. What form would make this knowledge accessible and easy to apply? How can we learn from previous errors and make proven, working solutions to recurring problems available to everyone?

The approach in this book is to apply the idea of *patterns*, which are an established software development technique. The basic idea behind patterns is to capture expert knowledge in the form of documentation with a specific structure containing proven solutions for recurring problems in a given domain. In particular, security patterns can be used when the people responsible for enterprises or systems have little or no security expertise. This allows them to address basic security issues themselves, instead of depending on security specialists to perform this task for them each time. This frees security specialists to help solve new or more complex security problems.

People will probably continue to develop and use second-class security solutions. Even relatively unskilled computer users, if they are intent on hacking, are able to carry out damaging attacks using widely-available scripts. Developing first-class solutions is an enormously difficult problem, exhibiting too many cases of inadequate requirements, ill-formed design concepts, poor architectures, inadequate specifications, immature software development practices, overdependence on system administration, poor operations, and uninformed top management. The earlier we start to treat security as an equivalent requirement with the appropriate priority, the quicker our know-how and skills about seamless security solutions will evolve. This would considerably

reduce the residual risk of using software applications and systems in sensitive environments. More and more we depend on having secure systems, and we need systematic solutions. Our belief is that security patterns are a step in this direction.

The Book's Intended Audiences

This book is intended for anyone who has a little knowledge of security but who needs to incorporate basic security functions into his organization or system, either because they are required to do so, or because they understand the importance of security. The book is also useful for specialists to use as a design guide, to compare systems, and to teach about systems.

In particular, we address the following audiences:

- At the enterprise level, everyone who is or should be interested in enterprise security, such as enterprise planners, enterprise architects, strategists, and policy makers, as well as business process engineers and business process re-engineering specialists. The main issue for these groups is to understand how to define basic enterprise security needs and constraints. Security patterns for this target group are presented in Chapter 6, *Enterprise Security and Risk Management*. We also recommend that they look at the patterns that are described in Chapters 7 to 13, to understand how enterprise security plans are reflected or satisfied in enterprise operations.
- At the IT system level, system architects, software designers and developers, project managers, product vendors, service suppliers and others interested in system security. These groups have to understand how to design basic system security functions and incorporate them into system architectures and designs, and how to select among alternative security solutions. We have compiled a set of corresponding security patterns in Chapters 7 to 13. At this level it is also important to understand the enterprise security constraints described in Chapter 6, *Enterprise Security and Risk Management*, and how they affect system security requirements.
- At an operational level, operations managers, operations staff, and other people interested in operations security. Their interest is to understand how to define and adopt basic security practices in enterprise and system operations. Relevant security patterns are discussed in Chapter 7, *Identification and Authentication (I&A)*, Chapter 10, *Operating System Access Control*, Chapter 11, *Accounting*, Chapter 12, *Firewall Architectures*, and Chapter 13, *Secure Internet Applications*.

It is clear that all these levels interact, and a complete understanding of security requires some degree of understanding of all of them.

There are further groups who may find the book useful, and can read any chapters of interest:

- Security specialists will be interested in comparing our security taxonomy with others. They may also want to see how familiar security solutions are represented in the form of patterns. They can also use or reference the patterns to reduce the number of times they have to repeat the same answers to the same security questions.
- Researchers, teachers, and students can use the book to understand current best practice in security. They may also find potential areas for extensions to our approach. For example, they could examine the security taxonomy to find areas not covered by current patterns. Advantages of security patterns for this target group could include their use in the design of new systems, understanding of complex systems, comparison of systems, and for teaching purposes: security patterns are used in university security courses, for example.
- Security auditors can improve their understanding using this new representation of best security practice. The collection of patterns also include *forces* and liabilities to watch for: in the Patterns community, we use the term 'forces' to describe goals and constraints that reveal the intricacies of a problem and define the kinds of trade-offs that must be considered in the presence of the tension or dissonance they create.
- Government acquisition or procurement specialists might get help in understanding a new representation of best security practice that can be included in an acquisition document such as a Request for Proposal or Statement of Work.

Structure of the Book

The first chapter, *The Pattern Approach*, provides a general introduction to the overall pattern paradigm. In addition to a discussion of the pattern approach, the chapter presents the pattern template we use in the book.

Chapter 2, *Security Foundations*, introduces key security concepts. We provide a general overview of security, followed by a taxonomy of security areas and a set of general security resources.

Applying patterns to the area of security results in a new, domain-specific pattern type: security patterns. In Chapter 3, *Security Patterns*, we outline how security patterns have evolved, and describe their distinguishing characteristics. We also discuss the benefits of using security patterns, and data sources for identifying security patterns.

Chapter 4, *Patterns Scope and Enterprise Security*, describes the scope and context of security patterns and explains how they are organized in the book.

Chapter 5, *The Security Pattern Landscape*, presents thumbnails for all the patterns in this book, as well as related security patterns that we reference, but are not contained in the book. In many cases these are published elsewhere.

Chapters 6 through 13 present the security patterns themselves.

In Chapter 6, *Enterprise Security and Risk Management*, we present security patterns at the enterprise level. These patterns emphasize the security considerations that planners need to incorporate into their development of enterprise-level strategy, planning activities, business models, goals, and policies.

Chapter 7, *Identification and Authentication (I&A)*, introduces service patterns that support aspects of the I&A service and selected individual patterns in this system. Identification and Authentication (I&A) services address the task of recognizing an actor—that is, a user, a process or any other system—that is interacting with a business system.

Chapter 8, *Access Control Models*, presents patterns that specify accepted access-control models as object-oriented, declarative patterns that can be used as guidelines in the construction of secure systems. There is also a pattern that documents the dynamics of evaluating requests according to the constraints defined by the declarative models. Finally, we also show a pattern that helps to find the rights associated with roles in a role-based access control (RBAC) model.

Chapter 9, *System Access Control Architecture*, presents access-control patterns at the architectural level. There is a pattern that shows why and how to gather the underlying requirements for a system under consideration from a generic set of access control requirements. The remainder of this chapter contains patterns that deal with the architecture of software systems to be secured by access control.

Chapter 10, *Operating System Access Control*, presents patterns for access control services and mechanisms targeted at operating systems that describe how the operating system controls access to resources such as memory address spaces and I/O devices.

Chapter 11, *Accounting*, presents patterns for audit and accounting services and mechanisms. Decision makers need to be aware of any security events that occur that involve their assets. This need is addressed by security audit and accounting patterns.

Chapter 12, *Firewall Architectures*, presents a pattern language for describing different types of firewalls. This language can be used as a guide to select a suitable firewall type for a system or to help designers build new firewalls.

Chapter 13, *Secure Internet Applications*, presents patterns for Internet security that specialize patterns from Chapter 8, *Access Control Models*, and Chapter 12, *Firewall Architectures*, within the domain of Internet applications.

Chapter 14, *Case Study: IP Telephony*, presents a case study of an emerging technology that demonstrates how to use security patterns to incorporate security into real-world system engineering scenarios. The most appropriate patterns of this book are applied to selected use cases in IP telephony systems.

Chapter 15, *Supplementary Concepts*, discusses selected complementary concepts that can be used in conjunction with security patterns. In particular, we present the pattern-related notion of security principles and so-called 'misuse cases.'

Chapter 16, *Closing Remarks*, provides our conclusions and an outlook on future work that deals with security patterns and related concepts.

Guidelines for the Reader

In addition to the obvious option of reading the book from cover to cover, you can choose alternative paths though the book.

This book is divided in three parts. The first part, which comprises Chapters 1 through 3, provides relevant background information about security patterns. If you are not familiar with patterns, read Chapter 1, *The Pattern Approach*, which contains a brief introduction to the ideas behind software patterns. If you are not familiar with security, read Chapter 2, *Security Foundations*, which provides basic concepts and pointers to sources of detailed security knowledge. Based on that, Chapter 3, *Security Patterns*, discusses the notion of security patterns.

The second part of the book, Chapters 4 through 13, contains a catalog of selected security patterns that address different topics. You can work through the catalog chapter by chapter to get an impression of typical security problems and proven solutions that occur at the different levels.

To understand how security patterns can be organized, read Chapter 4, *Patterns Scope and Enterprise Security*, which builds on our security taxonomy. If you want to get a quick overview of our security patterns, as well as related security patterns that are not presented in this book, read Chapter 5, *The Security Pattern Landscape*. This chapter can be used as a reference and a navigation tool.

Reading the patterns in Chapters 6 through 13 can be done in any desired sequence, or with any desired subset of the patterns. Within a given pattern, the key topics to read are *Context*, *Problem*, and *Solution*. The other parts of the patterns are optional and provide further information about implementing the pattern. We also identify the relationships between the patterns. You can therefore also start with any pattern and use the references to related patterns to navigate through the book.

If you have read the introductory chapters and security patterns are new to you, we suggest that you start with security patterns that are easy to understand and that are used in many situations. Examples are:

- Password Design and Use (217)
- Single Access Point (279)
- Front Door (473)

In the third part of the book we discuss applications, extensions and future directions of a pattern-based security approach. If you are looking for examples that describe how security patterns can be applied, look at the case study provided in

Chapter 14, *Case Study: IP Telephony*. If you are interested in techniques that can complement or augment the concept of security patterns, have a look at a few examples in Chapter 15, *Supplementary Concepts*. Conclusions and a look at the future of this work are given in Chapter 16, *Closing Remarks*. As these chapters build on the patterns in the book, you should read them last.

About the Authors

Many people contributed to this book. In this section we provide short biographies of all the authors and editors in alphabetical order. We also show briefly who contributed to which part of the book. Finally, we express our thanks to all the other people that helped to bring this book to a successful conclusion.

Short Biographies

Frank Buschmann

Frank Buschmann is Senior Principal Engineer at Siemens Corporate Technology in Munich, Germany. His research interests include object technology, software architecture, frameworks, and patterns. He has published widely in all these areas, most visibly in his co-authorship of the first two POSA volumes, *A System of Patterns* and *Patterns for Concurrent and Networked Objects*. Frank was a member of the ANSI C++ standardization committee X3J16 from 1992 to 1996. He initiated and organized the first conference on patterns held in Europe, EuroPLoP 1996, and is also a co-editor of the third book in the PLoPD series by Addison-Wesley. In his development work Frank has led design and implementation efforts for several large-scale industrial software projects, including business information, industrial automation, and telecommunication systems. In addition, Frank serves as the series editor for Wiley's series in software design patterns.

Susan Chapin

Susan Chapin has worked in research on information system technologies and issues relating to the management of security. She investigated the Windows NT/Windows 2000 operating system from an information security perspective, participated in the

development of a multi-level operating system for the Defense Information Systems Agency (DISA), and supported the development of high-level security architectures for the US Treasury Department, which included a focus on issues and uses of enterprise-wide directory services for the Internal Revenue Service (IRS). Some of her recent research has included studies of procedures to support the true integration of security into an enterprise architecture. Susan retired from MITRE in September 2003.

Nelly Delessy-Gassant

Nelly Delessy-Gassant is a Ph.D. student at Florida Atlantic University, working under the direction of Dr. Eduardo B. Fernandez. Her dissertation work is about trust in systems using Web Services. She is the author of several security patterns, for example in the area of firewalls.

Paul Dyson

Paul Dyson has built large-scale internet-based systems for a number of companies that include Philips, Lastminute.com, ThinkNatural.com and Interbrew. On these projects Paul has taken the role of application architect, designing both hardware and software architectures, as well as providing technical leadership to the development teams. He is a conference presenter and has chaired international events such as EuroPLoP and OT.

Ben Elsinga

Ben Elsinga is a specialist in information architecture and information security. He has carried out several assignments in the areas of risk analyses, security architecture, as well as acting as an interim security manager and a lecturer on information security courses. Within Capgemini Benelux, Ben led all research and information security development activities. He created a competence network of security specialists and consultants, and is member of the board of the Dutch information security society (GvIB). The vision Ben has is that information security should be integrated into every change, and that humans are the weakest link in the chain. He feels very comfortable in dynamic environments and from an innovative and result-driven attitude he likes to create new and secure business solutions. In an environment that contains the combination of system development and information security, Ben takes responsibility for a team of specialists to fulfill challenging assignments. He is a Capgemini certified senior IT architect, specialized in system development and information security. Ben successfully passed a B-screening by the Dutch government, and he is also a certified Prince-2 practitioner and is also a certified CISSP in information security.

Eduardo B. Fernandez

Eduardo B. Fernandez (Eduardo Fernandez-Buglioni) is a professor in the Department of Computer Science and Engineering at Florida Atlantic University in Boca Raton, Florida. He has published numerous papers on authorization models, object-oriented analysis and design, and fault-tolerant systems. He has written three books on these subjects. He has lectured all over the world at both academic and industrial meetings, and has created and taught several graduate and undergraduate courses and industrial tutorials. His current interests include security patterns and Web Services security. He holds an M.S. degree in Electrical Engineering from Purdue University and a Ph.D. in Computer Science from UCLA. He is a Senior Member of the IEEE, and a Member of ACM. He is an active consultant for industry, including assignments with IBM, Allied Signal, Motorola, Lucent, and others.

Mei Fullerton

Mei Fullerton recently completed her M.S. in Computer Science at Florida Atlantic University (May 2005). Since then she has worked as a software engineer at Office Depot, Delray Beach, Florida.

Manuel Görtz

Manuel Görtz is a researcher in the field of context-aware communication services. He holds an M.Sc. (Diplom) in Electrical Engineering and Information Technology from the Technischen Universität Darmstadt (TUD). He joined the Multimedia Communication Lab headed by Prof. Ralf Steinmetz at TUD in 2000. He recently received his Ph.D. in Electrical Engineering and Information Technology on the topic of 'Efficient Real-time Communication Services Utilizing Contexts.'

Manuel Görtz has actively working in the area of Voice over IP for many years. He was a member of the task-force that hosted the IP telephony trial for the Darmstadt scientific region, analyzing security threads and operational issues. He has worked for many years in industry projects to design and prototype communication solutions for the future. Manuel is an author of numerous peer-reviewed papers and several invention reports. His key expertise lies in the domain of signaling, advanced communication services and security patterns.

Jody Heaney

Jody Heaney is a Principle InfoSec Engineer in the Information Security Center at the MITRE Corporation in McLean, VA. She has been involved in many different program areas, including work with DARPA, the National Security Agency (NSA), all branches of the military, the Intelink Management Office (IMO), and the Intelligence

Community (IC). She has conducted research into the foundations of information assurance (IA) and has published papers on security modeling and access control. She was one of the original developers of the System Security Engineering Capability Maturity Model (CMM) and NSA's Information Assurance Technology Framework (IATF). In her current IA leadership role for the IC CIO, the focus is on identifying cross-cutting IA technologies suitable for the entire IC, especially for cross-security-domain technologies, and information sharing. She has maintained a strong interest in integrating information systems security into the mainstream of software and systems engineering processes.

Aaldert Hofman

Aaldert Hofman has elaborate knowledge and experience in sophisticated and complex information systems. He graduated in Informatics at Twente University in Enschede, the Netherlands and joined Capgemini in January 1990. During the first years of his career he was involved in the architecture of large administrative systems within social security. Since 1997 he has been assigned to projects in banking and insurance services. His expertise is in both architecture and security. He oversees the complexity in these fields and is able to align business to available IT resources. Aaldert is experienced in bridging the gap between business and IT both in his assignments and his coaching in architecture and security. Aaldert has been interested in the use of patterns since the famous GoF book on *Design Patterns*. Working in knowledge-intensive areas such as identity management and information security, he was convinced that knowledge capture by the use of patterns could be very helpful. He therefore joined the security patterns community during 2001, together with his colleague Ben Elsinga. They submitted security patterns to EuroPLoP 2002 and 2003, where they met the editors of this book and discussed their ideas. In their projects the use of security patterns has lead to better control of access rights, improving quality and time-to-market.

Duane Hybertson

Duane Hybertson is a researcher and member of the technical staff in the Center for Innovative Computing and Informatics at the MITRE Corporation in McLean, VA. He has a broad background in software engineering, both in research and practice. He has conducted research into the foundations of systems architecture, and has published papers on a uniform modeling approach to architecture and software engineering. He has supported architecture development and helped to define evolutionary processes for large information systems at the National Geospatial-Intelligence Agency (NGA), which supports both the US Department of Defense (DoD) and the intelligence community. He has applied architecture and modeling concepts to enterprise engineering, and is extending the model-oriented approach to complex systems.

His recent research has been in capturing security patterns and determining how to integrate these patterns into a usable enterprise engineering context.

Malcolm Kirwan, Jr.

Malcolm Kirwan, Jr. is a Lead Software Systems Engineer and Scientist at the MITRE Corporation in McLean, VA. Malcolm has spent his career performing activities throughout all phases of the systems and software development lifecycles. His experience ranges from designing and developing software for real-time embedded systems and simulation systems, to designing and incorporating security solutions into enterprise and system architectures.

Maria M. Larrondo-Petrie

Dr. Larrondo-Petrie is Associate Dean of Engineering and Professor of Computer Science & Engineering at Florida Atlantic University (FAU), and a member of the Secure Systems Research Group at FAU. She serves on the ASEE Minority Division Board, is Vice President of Research of the Latin American and Caribbean Consortium of Engineering Institutions, was on the ACM SIGGRAPH Education Board and was President of Upsilon Pi Epsilon Honor Society for the Computing Sciences.

Andy Longshaw

Andy Longshaw is an independent consultant, writer and educator specializing in enterprise platforms (both .NET and J2EE), Web-based technologies, Web Services, and components, particularly the design and architectural decisions required to use these technologies successfully. In recent years, Andy has worked on Internet technology projects and architecture for organizations such as Tesco Stores and Barclays Bank.

Andreas L. Opdahl

Andreas L. Opdahl is Professor of Information Systems Development at the Department of Information Science and Media Studies, University of Bergen, Norway. He is the author, co-author or co-editor of more than fifty journal articles, book chapters, refereed archival conference papers and books on multi-perspective enterprise modeling, requirements engineering, information systems architecture, software performance engineering and other areas. He serves regularly as a reviewer for premier international journals and on the program committees of renowned international conferences and workshops, and is a member of IFIP WG8.1 on Design and Evaluation of Information Systems.

Ann Reedy

Ann Reedy is a researcher and member of the technical staff in the Center for Innovative Computing and Informatics at the MITRE Corporation in McLean, VA. She has a broad background in both software engineering and enterprise architecture. She has supported the development of both enterprise architecture frameworks and enterprise architectures for DoD and a broad range of civil agencies. In addition to her recent research work on security patterns at MITRE, she has been working with Syracuse University in integrating security and enterprise engineering concepts in support of the Federal Enterprise Architecture Security and Privacy Profile. She is currently involved in providing enterprise architecture courses through the MITRE Institute and the Federal Enterprise Architecture Certification Institute.

Naeem Seliya

Naeem Seliya completed his Ph.D. in Computer Science at Florida Atlantic University in July 2005. His dissertation work was about the classification of error-prone software modules.

Sasha Romanosky

Sasha Romanosky, CISSP, holds a Bachelor of Science degree in Electrical Engineering from the University of Calgary, Canada and is currently pursuing graduate studies in Information Security at Carnegie Mellon. Sasha has been working with Internet and security technologies for over eight years, predominantly within the financial and e-commerce industries at companies such as Morgan Stanley and eBay. He coauthored the book *J2EE Design Patterns Applied* and has published other works on security patterns. Recently, Sasha collaborated with other leading industry professionals to develop the Common Vulnerability Scoring System (CVSS), an open framework for scoring computer vulnerabilities. His current research interests include vulnerability management and security metrics. His passion is information security. Sasha would like to thank his shepherds Duane Hybertson and Aaldert Hofman, as well as Markus Schumacher, for his vision in this book. Finally, Sasha would like to thank Theresa for her never-ending love and support.

Markus Schumacher

Markus Schumacher studied Electrical Engineering and Information Technology at the Darmstadt University of Technology (TUD). After finishing his studies in 1998, he was the leader of the IT Transfer Office (ITO) team that was—and still is—engaged in numerous national and international research projects in cooperation with well-known companies and public institutions that include SAP AG, T-Systems, Fujitsu