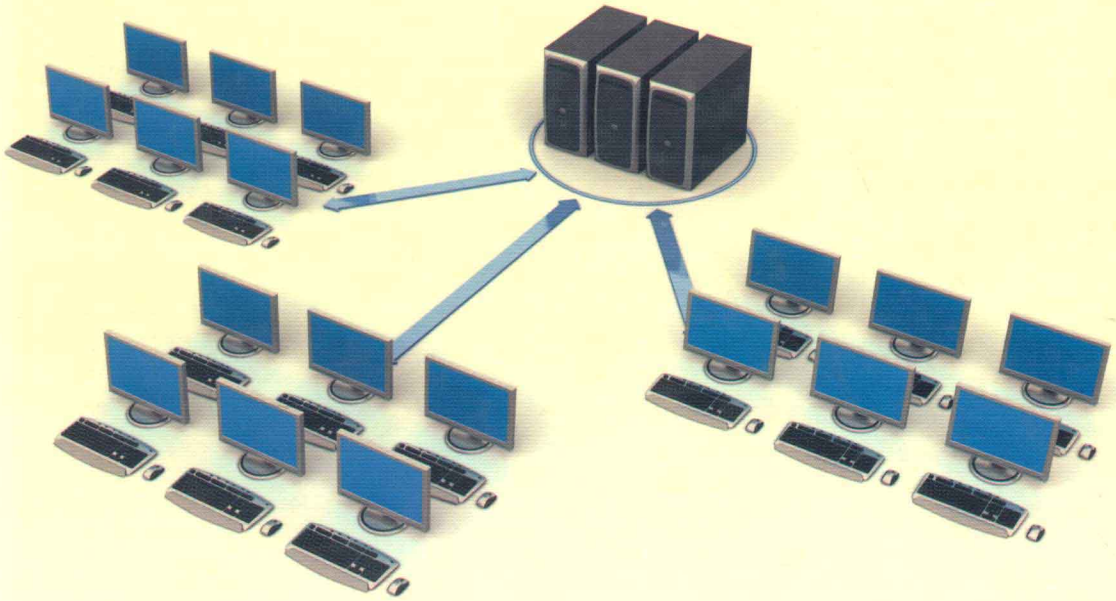
INFORMATION SECURITY SERIES

“十二五”国家重点图书出版规划项目



Shuangbao (Paul) Wang
Robert S. Ledley

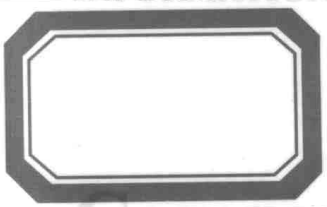
Computer Architecture and Security

计算机体系结构与安全

高等教育出版社
HIGHER EDUCATION PRESS

“十二五”国家重点图书出版规划项目

INFORMATION SECURITY SERIES



Computer Architecture and Security

计算机体系结构与安全

JISUANJI TIXI JIEGOU YU ANQUAN

Shuangbao (Paul) Wang
Robert S. Ledley

高等教育出版社·北京
HIGHER EDUCATION PRESS BEIJING

图书在版编目(CIP)数据

计算机体系结构与安全 = Computer Architecture and Security : 英文 / 王双保, (美) 莱德利 (Ledley, R. S.) 著. — 北京 : 高等教育出版社, 2013.1
(信息安全系列)
ISBN 978-7-04-034492-9

Ⅰ. ①计… Ⅱ. ①王…②莱… Ⅲ. ①计算机体系结构-系统安全性-研究-英文 Ⅳ. ①TP303②TP309

中国版本图书馆CIP数据核字(2012)第252944号

策划编辑 陈红英 责任编辑 陈红英 封面设计 张 楠 版式设计 杜微言
责任印制 朱学忠

出版发行	高等教育出版社	咨询电话	400-810-0598
社 址	北京市西城区德外大街4号	网 址	http://www.hep.edu.cn
邮政编码	100120		http://www.hep.com.cn
印 刷	涿州市星河印刷有限公司	网上订购	http://www.landraco.com
开 本	787mm×1092mm 1/16		http://www.landraco.com.cn
印 张	21.5	版 次	2013年1月第1版
字 数	490千字	印 次	2013年1月第1次印刷
购书热线	010-58581118	定 价	69.00元

物料号 34492-00

“十二五”国家重点图书出版规划项目

INFORMATION SECURITY SERIES

INFORMATION SECURITY SERIES

Information Security Series systematically introduces the fundamentals of information security design and application. The goals of the Series are:

- to provide fundamental and emerging theories and techniques to stimulate more research in cryptology, algorithms, protocols, and architectures
- to inspire professionals to understand the issues behind important security problems and the ideas behind the solutions
- to give references and suggestions for additional reading and further study

Publications consist of advanced textbooks for graduate students as well as researcher and practitioner references covering the key areas, including but not limited to:

— Modern Cryptography
— Cryptographic Protocols and Network Security Protocols
— Computer Architecture and Security
— Database Security
— Multimedia Security
— Computer Forensics
— Intrusion Detection

LEAD EDITORS

EDITORIAL BOARD

About the Authors

Shuangbao (Paul) Wang is the inventor of a secure computer system. He is the recipient of Link Fellowship Award in advanced simulation and training. He holds four patents; three of them have been transferred into industry and put into production. One of his students appeared in *Time Magazine* for doing his class project which he commercialized and still pursues. In addition, one of his published papers ranked the first place in Science Direct's TOP 25 Hottest Articles. His research was awarded the Best Invention Award in Entrepreneurship Week USA at Mason. More recently, he received two University Technology Transfer Awards.

Dr. Wang has extensive experience in academia, industry, and public services. He has held many posts, including professor, director, CEO, CIO/CTO and ranking positions in public services. He is currently a professor at George Mason University. Dr. Wang served as the Chief Information and Technology Officer at National Biomedical Research Foundation (USA) /Georgetown University Medical Center. Earlier, he was the director of the Institute of Information Science and Technology at Qingdao (ISTIQ) where he oversaw more than 120 faculty and staff, acquired 12 grants, won 18 academic awards and was the PI for over 15 grants/projects.

Robert S. Ledley is the inventor of CT scanner and is a member of the National Academy of Science (USA). He has numerous publications in *Science* and several books, and has hundreds of patents and grants. Dr. Ledley is the recipient of the National Medal of Technology (USA) that was awarded to him by President Clinton in 1997. He was admitted to the National Inventors Hall of Fame in 1990.

Dr. Ledley has been the president of the National Biomedical Research Foundation (USA) since 1960. He is also a professor (emeritus) at Georgetown University. Dr. Ledley is the editor-in-chief of four international journals. He has testified before the House and was interviewed by the Smithsonian Institution.

To our parents who care and educate us throughout our journey.

In memory of Dr. Ledley, who pioneered Biomedical Computing.

Preface

This book provides the fundamentals of computer architecture and security. It covers a wide range of computer hardware, system software and data concepts from a security perspective. It is essential for computer and information security professionals to understand both hardware and software security solutions to thrive in the workplace. It features a careful, in-depth, and innovative introduction to modern computer systems and patent-pending technologies in computer security.

In the past, computers were designed without security considerations. Later, firewalls were used to protect them from outside attacks. This textbook integrates security considerations into computer architecture in a way that it is immune from attacks. When necessary, the author creates simplified examples from patent-pending technologies that clearly explain architectural and implementation features.

This book is intended for graduate and undergraduate students, engineers, and researchers who are interested in secure computer architecture and systems. This book is essential for anyone who needs to understand, design or implement a secure computer system.

Studying computer architecture from a security perspective is a new area. There are many textbooks about computer architecture and many others about computer security. However, textbooks introducing computer architecture with security as the main theme are rare. This book introduces not only how to secure computer components (Memory, I/O, network interfaces and CPU) but also how to secure the entire computer system. The book proposes a new model that changes the Neumann architecture that has been the foundation of modern computers since 1945. The book includes the most recent patent-pending technology in computer architecture for security. It also incorporates experiences from the author's recent award-winning teaching and research.

This book also introduces the latest technologies, such as virtualization, cloud computing, Internet computing, ubiquitous computing, biocomputers and other advanced computer architectures, into the classroom in order to shorten the transition time from student to employee.

This book has a unique style of presentation. It uses diagrams to explain important concepts. For many key elements, the book illustrates the actual digital circuits so that interested readers can actually build such circuits for testing purposes. The book can also be used as experiment material.

The book also comes with a Wiley Companion Website (www.wiley.com/go/wang/comp_arch) that provides lecture notes, further readings and updates for students. It also provides resources for instructors as well. In addition, the website lists hundreds of security tools that can be used to test computers for security problems.

Students taking courses with this book can master security solutions in all aspects of designing modern computer systems. It introduces how to secure memory, buses, I/O and CPU. Moreover, the book explains how to secure computer architecture so that modern computers can be built on the new architecture free of data breaches.

The concept of computers as stand-alone machines is fading away. Computers are now interconnected and in many cases coordinated to accomplish one task. Most current computer architecture textbooks still focus on the single computer model without addressing any security issues. *Computer Architecture and Security* provides readers with all of the components the traditional textbooks have, but also the latest development of computer technology. As security is a concern for most people, this book addresses the security issues in depth in all aspects of computer systems.

Acknowledgements

The authors would like to thank Dr. and Mrs. McQuivey for the thorough reviews and editions. Dr. Kyle Letimar provided tremendous help in editing and revising the book proposal. The authors would also like to acknowledge Ms. Anna Chen for her incredible help in preparing this manuscript.

Contents

* The star "*" here means the content is a little bit more advanced. For teaching purpose, this content may be omitted for entry level students.