

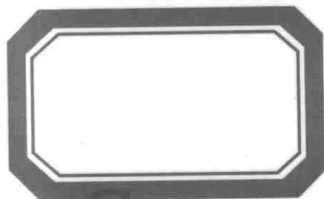
Shuangbao (Paul) Wang  
Robert S. Ledley

# Computer Architecture and Security

计算机体系结构与安全

“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

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	<a href="http://www.hep.edu.cn">http://www.hep.edu.cn</a>
邮政编码	100120		<a href="http://www.hep.com.cn">http://www.hep.com.cn</a>
印 刷	涿州市星河印刷有限公司	网上订购	<a href="http://www.landaco.com">http://www.landaco.com</a>
开 本	787mm×1092mm 1/16		<a href="http://www.landaco.com.cn">http://www.landaco.com.cn</a>
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

本书如有缺页、倒页、脱页等质量问题,请到所购图书销售部门联系调换

版权所有 侵权必究

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

Song Y. Yan	London, UK
Moti Yung	Columbia University, USA
John Rief	Duke University, USA

## EDITORIAL BOARD

Liz Bacon	University of Greenwich, UK
Kefei Chen	Shanghai Jiaotong University, China
Matthew Franklin	University of California, USA
Dieter Gollmann	Hamburg University of Technology, Germany
Yongfei Han	Beijing University of Technology, China
	ONETS Wireless & Internet Security Tech. Co., Ltd. Singapore
Kwangjo Kim	KAIST-ICC, Korea
David Naccache	Ecole Normale Supérieure, France
Dingyi Pei	Guangzhou University, China
Peter Wild	University of London, UK

# 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](http://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

<b>1</b>	<b>Introduction to Computer Architecture and Security</b>	<b>1</b>
1.1	History of Computer Systems	3
1.1.1	<i>Timeline of Computer History</i>	5
1.1.2	<i>Timeline of Internet History</i>	15
1.1.3	<i>Timeline of Computer Security History</i>	28
1.2	John von Neumann Computer Architecture	34
1.3	Memory and Storage	36
1.4	Input/Output and Network Interface	37
1.5	Single CPU and Multiple CPU Systems	38
1.6	Overview of Computer Security	41
1.6.1	<i>Confidentiality</i>	41
1.6.2	<i>Integrity</i>	42
1.6.3	<i>Availability</i>	42
1.6.4	<i>Threats</i>	43
1.6.5	<i>Firewalls</i>	43
1.6.6	<i>Hacking and Attacks</i>	44
1.7	Security Problems in Neumann Architecture	46
1.8	Summary	48
	Exercises	48
	References	50
<b>2</b>	<b>Digital Logic Design</b>	<b>51</b>
2.1	Concept of Logic Unit	51
2.2	Logic Functions and Truth Tables	52
2.3	Boolean Algebra	54
2.4	Logic Circuit Design Process	55

2.5	Gates and Flip-Flops	56
2.6	Hardware Security	58
2.7	FPGA and VLSI	58
2.7.1	<i>Design of an FPGA Biometric Security System</i>	59
2.7.2	<i>A RIFD Student Attendance System</i>	59
2.8	Summary	65
	Exercises	67
	References	67
<b>3</b>	<b>Computer Memory and Storage</b>	<b>68</b>
3.1	A One Bit Memory Circuit	68
3.2	Register, MAR, MDR and Main Memory	70
3.3	Cache Memory	72
3.4	Virtual Memory	74
3.4.1	<i>Paged Virtual Memory*</i>	75
3.4.2	<i>Segmented Virtual Memory*</i>	75
3.5	Non-Volatile Memory	76
3.6	External Memory	77
3.6.1	<i>Hard Disk Drives</i>	78
3.6.2	<i>Tertiary Storage and Off-Line Storage*</i>	78
3.6.3	<i>Serial Advanced Technology Attachment (SATA)</i>	79
3.6.4	<i>Small Computer System Interface (SCSI)</i>	80
3.6.5	<i>Serial Attached SCSI (SAS)</i>	81
3.6.6	<i>Network-Attached Storage (NAS)*</i>	82
3.6.7	<i>Storage Area Network (SAN)*</i>	83
3.6.8	<i>Cloud Storage</i>	85
3.7	Memory Access Security	86
3.8	Summary	88
	Exercises	89
	References	89
<b>4</b>	<b>Bus and Interconnection</b>	<b>90</b>
4.1	System Bus	90
4.1.1	<i>Address Bus</i>	91
4.1.2	<i>Data Bus</i>	93
4.1.3	<i>Control Bus</i>	93
4.2	Parallel Bus and Serial Bus	95
4.2.1	<i>Parallel Buses and Parallel Communication</i>	95
4.2.2	<i>Serial Bus and Serial Communication</i>	96
4.3	Synchronous Bus and Asynchronous Bus	107

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

4.4	Single Bus and Multiple Buses	109
4.5	Interconnection Buses	110
4.6	Security Considerations for Computer Buses	111
4.7	A Dual-Bus Interface Design	112
4.7.1	<i>Dual-Channel Architecture*</i>	113
4.7.2	<i>Triple-Channel Architecture*</i>	114
4.7.3	<i>A Dual-Bus Memory Interface</i>	115
4.8	Summary	115
	Exercises	117
	References	117
<b>5</b>	<b>I/O and Network Interface</b>	<b>118</b>
5.1	Direct Memory Access	118
5.2	Interrupts	120
5.3	Programmed I/O	121
5.4	USB and IEEE 1394	122
5.4.1	<i>USB Advantages</i>	123
5.4.2	<i>USB Architecture</i>	123
5.4.3	<i>USB Version History</i>	124
5.4.4	<i>USB Design and Architecture*</i>	125
5.4.5	<i>USB Mass Storage</i>	127
5.4.6	<i>USB Interface Connectors</i>	128
5.4.7	<i>USB Connector Types</i>	130
5.4.8	<i>USB Power and Charging</i>	133
5.4.9	<i>IEEE 1394</i>	136
5.5	Network Interface Card	136
5.5.1	<i>Basic NIC Architecture</i>	137
5.5.2	<i>Data Transmission</i>	138
5.6	Keyboard, Video and Mouse (KVM) Interfaces	139
5.6.1	<i>Keyboards</i>	140
5.6.2	<i>Video Graphic Card</i>	140
5.6.3	<i>Mouses</i>	140
5.7	Input/Output Security	140
5.7.1	<i>Disable Certain Key Combinations</i>	141
5.7.2	<i>Anti-Glare Displays</i>	141
5.7.3	<i>Adding Password to Printer</i>	141
5.7.4	<i>Bootable USB Ports</i>	141
5.7.5	<i>Encrypting Hard Drives</i>	141
5.8	Summary	141
	Exercises	142
	References	143

<b>6</b>	<b>Central Processing Unit</b>	<b>144</b>
6.1	The Instruction Set	144
6.1.1	<i>Instruction Classifications</i>	144
6.1.2	<i>Logic Instructions</i>	145
6.1.3	<i>Arithmetic Instructions</i>	145
6.1.4	<i>Intel 64/32 Instructions*</i>	147
6.2	Registers	153
6.2.1	<i>General-Purpose Registers</i>	153
6.2.2	<i>Segment Registers</i>	155
6.2.3	<i>EFLAGS Register</i>	156
6.3	The Program Counter and Flow Control	158
6.3.1	<i>Intel Instruction Pointer*</i>	158
6.3.2	<i>Interrupt and Exception*</i>	159
6.4	RISC Processors	161
6.4.1	<i>History</i>	162
6.4.2	<i>Architecture and Programming</i>	162
6.4.3	<i>Performance</i>	163
6.4.4	<i>Advantages and Disadvantages</i>	163
6.4.5	<i>Applications</i>	164
6.5	Pipelining	164
6.5.1	<i>Different Types of Pipelines</i>	164
6.5.2	<i>Pipeline Performance Analysis</i>	165
6.5.3	<i>Data Hazard</i>	166
6.6	CPU Security	166
6.7	Virtual CPU	168
6.8	Summary	169
	Exercises	170
	References	170
<b>7</b>	<b>Advanced Computer Architecture</b>	<b>172</b>
7.1	Multiprocessors	172
7.1.1	<i>Multiprocessing</i>	172
7.1.2	<i>Cache</i>	173
7.1.3	<i>Hyper-Threading</i>	174
7.1.4	<i>Symmetric Multiprocessing</i>	175
7.1.5	<i>Multiprocessing Operating Systems</i>	175
7.1.6	<i>The Future of Multiprocessing</i>	176
7.2	Parallel Processing	177
7.2.1	<i>History of Parallel Processing</i>	177
7.2.2	<i>Flynn's Taxonomy</i>	178
7.2.3	<i>Bit-Level Parallelism</i>	178

7.2.4	<i>Instruction-Level Parallelism</i>	179
7.2.5	<i>Data-Level Parallelism</i>	179
7.2.6	<i>Task-Level Parallelism</i>	179
7.2.7	<i>Memory in Parallel Processing</i>	180
7.2.8	<i>Specialized Parallel Computers</i>	181
7.2.9	<i>The Future of Parallel Processing</i>	182
7.3	<i>Ubiquitous Computing</i>	182
7.3.1	<i>Ubiquitous Computing Development</i>	183
7.3.2	<i>Basic forms of Ubiquitous Computing</i>	184
7.3.3	<i>Augmented Reality</i>	185
7.3.4	<i>Mobile Computing</i>	186
7.4	<i>Grid, Distributed and Cloud Computing</i>	187
7.4.1	<i>Characteristics of Grid Computing</i>	187
7.4.2	<i>The Advantages and Disadvantages of Grid Computing</i>	188
7.4.3	<i>Distributed Computing</i>	189
7.4.4	<i>Distributed Systems</i>	189
7.4.5	<i>Parallel and Distributed Computing</i>	190
7.4.6	<i>Distributed Computing Architectures</i>	190
7.4.7	<i>Cloud Computing</i>	192
7.4.8	<i>Technical Aspects of Cloud Computing</i>	193
7.4.9	<i>Security Aspects of Cloud Computing</i>	194
7.4.10	<i>Ongoing and Future Elements in Cloud Computing</i>	195
7.4.11	<i>Adoption of Cloud Computing Industry Drivers</i>	196
7.5	<i>Internet Computing</i>	197
7.5.1	<i>Internet Computing Concept and Model</i>	198
7.5.2	<i>Benefit of Internet Computing for Businesses</i>	199
7.5.3	<i>Examples of Internet Computing</i>	201
7.5.4	<i>Migrating Internet Computing</i>	202
7.6	<i>Virtualization</i>	203
7.6.1	<i>Types of Virtualization</i>	203
7.6.2	<i>History of Virtualization</i>	205
7.6.3	<i>Virtualization Architecture</i>	205
7.6.4	<i>Virtual Machine Monitor</i>	207
7.6.5	<i>Examples of Virtual Machines</i>	207
7.7	<i>Biocomputers</i>	209
7.7.1	<i>Biochemical Computers</i>	209
7.7.2	<i>Biomechanical Computers</i>	209
7.7.3	<i>Bioelectronic Computers</i>	210
7.8	<i>Summary</i>	211
	<i>Exercises</i>	212
	<i>References</i>	214

<b>8</b>	<b>Assembly Language and Operating Systems</b>	<b>216</b>
8.1	Assembly Language Basics	217
8.1.1	<i>Numbering Systems</i>	217
8.1.2	<i>The Binary Numbering System and Base Conversions</i>	219
8.1.3	<i>The Hexadecimal Numbering System</i>	220
8.1.4	<i>Signed and Unsigned Numbers</i>	221
8.2	Operation Code and Operands	223
8.3	Direct Addressing	225
8.4	Indirect Addressing	225
8.5	Stack and Buffer Overflow	226
8.5.1	<i>Calling Procedures Using CALL and RET (Return)</i>	228
8.5.2	<i>Exploiting Stack Buffer Overflows</i>	229
8.5.3	<i>Stack Protection</i>	231
8.6	FIFO and M/M/1 Problem	232
8.6.1	<i>FIFO Data Structure</i>	232
8.6.2	<i>M/M/1 Model</i>	233
8.7	Kernel, Drivers and OS Security	234
8.7.1	<i>Kernel</i>	234
8.7.2	<i>BIOS</i>	235
8.7.3	<i>Boot Loader</i>	236
8.7.4	<i>Device Drivers</i>	237
8.8	Summary	238
	Exercises	239
	References	240
<b>9</b>	<b>TCP/IP and Internet</b>	<b>241</b>
9.1	Data Communications	241
9.1.1	<i>Signal, Data, and Channels</i>	242
9.1.2	<i>Signal Encoding and Modulation</i>	243
9.1.3	<i>Shannon Theorem</i>	244
9.2	TCP/IP Protocol	244
9.2.1	<i>Network Topology</i>	245
9.2.2	<i>Transmission Control Protocol (TCP)</i>	246
9.2.3	<i>The User Datagram Protocol (UDP)</i>	247
9.2.4	<i>Internet Protocol (IP)</i>	247
9.3	Network Switches	248
9.3.1	<i>Layer 1 Hubs</i>	248
9.3.2	<i>Ethernet Switch</i>	249
9.4	Routers	250
9.4.1	<i>History of Routers</i>	251
9.4.2	<i>Architecture</i>	251
9.4.3	<i>Internet Protocol Version 4 (IPv4)</i>	253



9.4.4	<i>Internet Protocol Version 6 (IPv6)</i>	254
9.4.5	<i>Open Shortest Path First</i>	254
9.4.6	<i>Throughput and Delay</i>	256
9.5	Gateways	257
9.6	Wireless Networks and Network Address Translation (NAT)	258
9.6.1	<i>Wireless Networks</i>	258
9.6.2	<i>Wireless Protocols</i>	260
9.6.3	<i>WLAN Handshaking, War Driving, and WLAN Security</i>	261
9.6.4	<i>Security Measures to Reduce Wireless Attacks</i>	263
9.6.5	<i>The Future of Wireless Network</i>	263
9.6.6	<i>Network Address Translation</i>	264
9.6.7	<i>Environmental and Health Concerns Using Cellular and Wireless Devices</i>	265
9.7	Network Security	267
9.7.1	<i>Introduction</i>	268
9.7.2	<i>Firewall Architecture</i>	271
9.7.3	<i>Constraint and Limitations of Firewall</i>	273
9.7.4	<i>Enterprise Firewalls</i>	274
9.8	Summary	275
	Exercises	276
9.9	Virtual Cyber-Security Laboratory	277
	References	278
<b>10</b>	<b>Design and Implementation: Modifying Neumann Architecture</b>	<b>280</b>
10.1	Data Security in Computer Systems	280
10.1.1	<i>Computer Security</i>	281
10.1.2	<i>Data Security and Data Bleaches</i>	282
10.1.3	<i>Researches in Architecture Security</i>	283
10.2	Single-Bus View of Neumann Architecture	284
10.2.1	<i>John von Neumann Computer Architecture</i>	284
10.2.2	<i>Modified Neumann Computer Architecture</i>	285
—10.2.3	<i>Problems Exist in John Neumann Model</i>	286
10.3	A Dual-Bus Solution	286
10.4	Bus Controller	288
10.4.1	<i>Working Mechanism of the Bus Controller</i>	288
10.4.2	<i>Co-processor Board</i>	289
10.5	Dual-Port Storage	292
10.6	Micro-Operating System	292
10.7	Summary	293
	Exercises	294
10.8	Projects	295
	References	295