

Principles of Secure Processor Architecture Design

Synthesis Lectures on Computer Architecture

Editor

Margaret Martonosi, *Princeton University*

Founding Editor Emeritus

Mark D. Hill, *University of Wisconsin, Madison*

Synthesis Lectures on Computer Architecture publishes 50- to 100-page publications on topics pertaining to the science and art of designing, analyzing, selecting and interconnecting hardware components to create computers that meet functional, performance and cost goals. The scope will largely follow the purview of premier computer architecture conferences, such as ISCA, HPCA, MICRO, and ASPLOS.

Principles of Secure Processor Architecture Design

Jakub Szefer
2018

General-Purpose Graphics Processor Architectures

Tor M. Aamodt, Wilson Wai Lun Fung, and Timothy G. Rogers
2018

Compiling Algorithms for Heterogenous Systems

Steven Bell, Jing Pu, James Hegarty, and Mark Horowitz
2018

Architectural and Operating System Support for Virtual Memory

Abhishek Bhattacharjee and Daniel Lustig
2017

Deep Learning for Computer Architects

Brandon Reagen, Robert Adolf, Paul Whatmough, Gu-Yeon Wei, and David Brooks
2017

On-Chip Networks, Second Edition

Natalie Enright Jerger, Tushar Krishna, and Li-Shiuan Peh
2017

Space-Time Computing with Temporal Neural Networks

James E. Smith
2017

Hardware and Software Support for Virtualization

Edouard Bugnion, Jason Nieh, and Dan Tsafir
2017

Datacenter Design and Management: A Computer Architect's Perspective

Benjamin C. Lee
2016

A Primer on Compression in the Memory Hierarchy

Somayeh Sardashti, Angelos Arelakis, Per Stenström, and David A. Wood
2015

Research Infrastructures for Hardware Accelerators

Yakun Sophia Shao and David Brooks
2015

Analyzing Analytics

Rajesh Bordawekar, Bob Blainey, and Ruchir Puri
2015

Customizable Computing

Yu-Ting Chen, Jason Cong, Michael Gill, Glenn Reinman, and Bingjun Xiao
2015

Die-stacking Architecture

Yuan Xie and Jishen Zhao
2015

Single-Instruction Multiple-Data Execution

Christopher J. Hughes
2015

Power-Efficient Computer Architectures: Recent Advances

Magnus Sjalander, Margaret Martonosi, and Stefanos Kaxiras
2014

FPGA-Accelerated Simulation of Computer Systems

Hari Angepat, Derek Chiou, Eric S. Chung, and James C. Hoe
2014

[A Primer on Hardware Prefetching](#)

Babak Falsafi and Thomas F. Wenisch

2014

[On-Chip Photonic Interconnects: A Computer Architect's Perspective](#)

Christopher J. Nitta, Matthew K. Farrens, and Venkatesh Akella

2013

[Optimization and Mathematical Modeling in Computer Architecture](#)

Tony Nowatzki, Michael Ferris, Karthikeyan Sankaralingam, Cristian Estan, Nilay Vaish, and David Wood

2013

[Security Basics for Computer Architects](#)

Ruby B. Lee

2013

[The Datacenter as a Computer: An Introduction to the Design of Warehouse-Scale Machines, Second Edition](#)

Luiz André Barroso, Jimmy Clidaras, and Urs Hölzle

2013

[Shared-Memory Synchronization](#)

Michael L. Scott

2013

[Resilient Architecture Design for Voltage Variation](#)

Vijay Janapa Reddi and Meeta Sharma Gupta

2013

[Multithreading Architecture](#)

Mario Nemirovsky and Dean M. Tullsen

2013

[Performance Analysis and Tuning for General Purpose Graphics Processing Units \(GPGPU\)](#)

Hyesoon Kim, Richard Vuduc, Sara Baghsorkhi, Jee Choi, and Wen-mei Hwu

2012

[Automatic Parallelization: An Overview of Fundamental Compiler Techniques](#)

Samuel P. Midkiff

2012

[Phase Change Memory: From Devices to Systems](#)

Moinuddin K. Qureshi, Sudhanva Gurusurthi, and Bipin Rajendran

2011

Multi-Core Cache Hierarchies

Rajeev Balasubramonian, Norman P. Jouppi, and Naveen Muralimanohar
2011

A Primer on Memory Consistency and Cache Coherence

Daniel J. Sorin, Mark D. Hill, and David A. Wood
2011

Dynamic Binary Modification: Tools, Techniques, and Applications

Kim Hazelwood
2011

Quantum Computing for Computer Architects, Second Edition

Tzvetan S. Metodi, Arvin I. Faruque, and Frederic T. Chong
2011

High Performance Datacenter Networks: Architectures, Algorithms, and Opportunities

Dennis Abts and John Kim
2011

Processor Microarchitecture: An Implementation Perspective

Antonio González, Fernando Latorre, and Grigorios Magklis
2010

Transactional Memory, Second Edition

Tim Harris, James Larus, and Ravi Rajwar
2010

Computer Architecture Performance Evaluation Methods

Lieven Eeckhout
2010

Introduction to Reconfigurable Supercomputing

Marco Lanzagorta, Stephen Bique, and Robert Rosenberg
2009

On-Chip Networks

Natalie Enright Jerger and Li-Shiuan Peh
2009

The Memory System: You Can't Avoid It, You Can't Ignore It, You Can't Fake It

Bruce Jacob
2009

Fault Tolerant Computer Architecture

Daniel J. Sorin

2009

The Datacenter as a Computer: An Introduction to the Design of Warehouse-Scale Machines

Luiz André Barroso and Urs Hölzle

2009

Computer Architecture Techniques for Power-Efficiency

Stefanos Kaxiras and Margaret Martonosi

2008

Chip Multiprocessor Architecture: Techniques to Improve Throughput and Latency

Kunle Olukotun, Lance Hammond, and James Laudon

2007

Transactional Memory

James R. Larus and Ravi Rajwar

2006

Quantum Computing for Computer Architects

Tzvetan S. Metodi and Frederic T. Chong

2006

© Springer Nature Switzerland AG 2022
Reprint of original edition ©Morgan & Claypool 2019

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopy, recording, or any other except for brief quotations in printed reviews, without the prior permission of the publisher.

Principles of Secure Processor Architecture Design
Jakub Szefer

ISBN: 978-3-031-00632-6	paperback
ISBN: 978-3-031-01760-5	ebook
ISBN: 978-3-031-00057-7	hardcover

DOI 10.1007/978-3-031-01760-5

A Publication in the Springer series
SYNTHESIS LECTURES ON COMPUTER ARCHITECTURE

Lecture #45
Series Editor: Margaret Martonosi, *Princeton University*
Founding Editor Emeritus: Mark D. Hill, *University of Wisconsin, Madison*
Series ISSN
Print 1935-3235 Electronic 1935-3243

Principles of Secure Processor Architecture Design

Jakub Szefer
Yale University

SYNTHESIS LECTURES ON COMPUTER ARCHITECTURE #45

ABSTRACT

With growing interest in computer security and the protection of the code and data which execute on commodity computers, the amount of hardware security features in today's processors has increased significantly over the recent years. No longer of just academic interest, security features inside processors have been embraced by industry as well, with a number of commercial secure processor architectures available today. This book aims to give readers insights into the principles behind the design of academic and commercial secure processor architectures. Secure processor architecture research is concerned with exploring and designing hardware features inside computer processors, features which can help protect confidentiality and integrity of the code and data executing on the processor. Unlike traditional processor architecture research that focuses on performance, efficiency, and energy as the first-order design objectives, secure processor architecture design has security as the first-order design objective (while still keeping the others as important design aspects that need to be considered).

This book aims to present the different challenges of secure processor architecture design to graduate students interested in research on architecture and hardware security and computer architects working in industry interested in adding security features to their designs. It aims to educate readers about how the different challenges have been solved in the past and what are the best practices, i.e., the principles, for design of new secure processor architectures. Based on the careful review of past work by many computer architects and security researchers, readers also will come to know the five basic principles needed for secure processor architecture design. The book also presents existing research challenges and potential new research directions. Finally, this book presents numerous design suggestions, as well as discusses pitfalls and fallacies that designers should avoid.

KEYWORDS

secure processor design, processor architecture, computer security, trustworthy computing, computer hardware security

Dla ukochanej Injoong i najwspanialszej Adusi.

Contents

	Preface	xix
	Acknowledgments	xxi
1	Introduction	1
1.1	Need for Secure Processor Architectures	1
1.2	Book Organization	3
2	Basic Computer Security Concepts	5
2.1	Trusted Computing Base	5
2.1.1	Kerckhoffs's Principle: Avoid Security through Obscurity	7
2.2	Security Threats to a System	7
2.2.1	The Attack Surface	7
2.2.2	Passive and Active Attacks	8
2.2.3	Man-In-The-Middle Attacks	9
2.2.4	Side and Covert Channels and Attacks	9
2.2.5	Information Flows and Attack Bandwidths	11
2.2.6	The Threat Model	11
2.2.7	Threats to Hardware After the Design Phase	12
2.3	Basic Security Concepts	13
2.3.1	Confidentiality, Integrity, and Availability	13
2.3.2	Authentication	15
2.3.3	Freshness and Nonces	15
2.3.4	Security vs. Reliability	15
2.4	Symmetric-Key Cryptography	16
2.4.1	Symmetric-Key Algorithms: Block Ciphers	16
2.4.2	Symmetric-Key Algorithms: Stream Ciphers	17
2.4.3	Standard Symmetric: Key Algorithms	17
2.5	Public-Key Cryptography	17
2.5.1	Key Encapsulation Mechanisms	18
2.5.2	Standard Public-Key Algorithms	18
2.5.3	Post-Quantum Cryptography	18

2.6	Random Number Generation	19
2.7	Secure Hashing	19
2.7.1	Use of Hashes in Message Authentication Codes	20
2.7.2	Use of Hashes in Digital Signatures	20
2.7.3	Use of Hashes in Hash Trees	20
2.7.4	Application of Hashes in Key Derivation Function	21
2.7.5	Standard Secure Hash Algorithms	21
2.8	Public Key Infrastructure	21
2.8.1	Digital Certificates	22
2.8.2	Diffie–Hellman Key Exchange	22
2.8.3	Application of PKI in Secure Processor Architectures	22
2.9	Physically Unclonable Functions	23
3	Secure Processor Architectures	25
3.1	Real-World Attacks	25
3.1.1	Coldboot	26
3.1.2	Rowhammer	26
3.1.3	Meltdown	27
3.1.4	Spectre	28
3.1.5	Other Bugs and Vulnerabilities	29
3.2	General-Purpose Processor Architectures	30
3.2.1	Typical Software Levels (Rings 3 to -1)	31
3.2.2	Typical Hardware Components	31
3.3	Secure Processor Architectures	32
3.3.1	Extending Vertical Privilege Levels	32
3.3.2	Horizontal Privilege Level Separation	34
3.3.3	Breaking Linear Hierarchy of Protection Levels	34
3.3.4	Capability-Based Protections	34
3.3.5	Architectures for Different Software Threats	34
3.3.6	Architectures for Different Hardware Threats	36
3.3.7	Hardware TCB as Circuits or Processors	37
3.4	Examples of Secure Processor Architectures	37
3.4.1	Academic Architectures	38
3.4.2	Commercial Architectures	39
3.5	Secure Processor Architecture Assumptions	39
3.5.1	Trusted Processor Chip Assumption	39
3.5.2	Small TCB Assumption	39

3.5.3	Open TCB Assumption	40
3.6	Limitations of Secure Architectures	40
3.6.1	Physical Realization Threats	40
3.6.2	Supply Chain Threats	40
3.6.3	IP Protection and Reverse Engineering	40
3.6.4	Side- and Covert-Channel Threats	41
3.6.5	What Secure Processor Architectures are Not	41
3.6.6	Alternatives to Hardware-Based Protections: Homomorphic Encryption	42
4	Trusted Execution Environments	43
4.1	Protecting Software within Trusted Execution Environments	43
4.1.1	Protections Offered by the TCB to the TEEs	43
4.1.2	Enforcing Confidentiality through Encryption	44
4.1.3	Enforcing Confidentiality through Isolation	44
4.1.4	Enforcing Confidentiality through State Flushing	46
4.1.5	Enforcing Integrity through Cryptographic Hashing	46
4.2	Examples of Architectures and TEEs	46
4.2.1	Academic Architectures for Protecting TSMs or Enclaves	47
4.2.2	Commercial Architectures for Protecting TSMs or Enclaves	48
4.2.3	Academic and Commercial Architectures for Protecting Whole OSes or VMs	49
4.3	TCB and TEE Assumptions	49
4.3.1	No Side Effects Assumption	49
4.3.2	Bug-Free Protected Software Assumption	49
4.3.3	Trustworthy TCB Execution Assumption	50
4.4	Limitations of TCBs and TEEs	50
4.4.1	Vulnerabilities in the TCB	50
4.4.2	Opaque TCB Execution	50
4.4.3	TEE-Based Attacks	51
4.4.4	TEE Code Bloat	51
5	Hardware Root of Trust	53
5.1	The Root of Trust	53
5.1.1	Root of Trust and the Processor Key	54
5.1.2	PKI and Secure Processors	54
5.1.3	Access to the Root of Trust	56

5.2	Chain of Trust and Measurements	56
5.2.1	Trusted and Authenticated Boot	57
5.2.2	Measurement Validation	58
5.2.3	Remote Attestation	58
5.2.4	Sealing	59
5.2.5	Time-of-Check to Time-of-Use Attacks	60
5.3	Runtime Attestation and Continuous Monitoring of TCB and TEEs	60
5.3.1	Limitations of Continuous Monitoring	61
5.4	PUFs and Root of Trust	61
5.4.1	Hardware-Software Binding	61
5.5	Limiting Execution to Only Authorized Code	62
5.5.1	Lock-in and Privacy Concerns	63
5.6	Root of Trust Assumptions	63
5.6.1	Unique of Root of Trust Key Assumption	63
5.6.2	Protected Root of Trust Assumption	63
5.6.3	Fresh Measurement Assumption	64
6	Memory Protections	65
6.1	Threats Against Main Memory	65
6.1.1	Sources of Attacks on Memory	65
6.1.2	Passive Attacks	66
6.1.3	Active Attacks	66
6.2	Main Memory Protection Mechanisms	67
6.2.1	Confidentiality Protection with Encryption	68
6.2.2	Integrity Protection with Hashing	70
6.2.3	Access Pattern Protection	73
6.3	Memory Protections Assumption	74
6.3.1	Encrypted, Hashed, and Oblivious Access Memory Assumption	74
7	Multiprocessor and Many-Core Protections	75
7.1	Security Challenges of Multiprocessors and Many-Core Systems	75
7.2	Multiprocessor Security	76
7.2.1	SMP and DSM Threat Model	76
7.2.2	Symmetric Memory Multiprocessor Security	77
7.2.3	Distributed Shared Memory Security	79
7.2.4	SMP and DSM Tradeoffs	80
7.3	Many-Core Processors and Multi-Processor System-on-a-Chip	81

7.3.1	Many-Core and MPSoC Threat Model	81
7.3.2	Communication Protection Mechanisms	82
7.3.3	3D Integration Considerations	83
7.4	Multiprocessor and Many-Core Protections Assumption	84
7.4.1	Protected Inter-Processor Communication Assumption	84
8	Side-Channel Threats and Protections	85
8.1	Side and Covert Channels	85
8.1.1	Covert Channel Review	85
8.1.2	Side Channel Review	86
8.1.3	Side and Covert Channels in Processors	87
8.2	Processor Features and Information Leaks	88
8.2.1	Variable Instruction Execution Timing	89
8.2.2	Functional Unit Contention	90
8.2.3	Stateful Functional Units	91
8.2.4	Memory Hierarchy	91
8.2.5	Physical Emanations	94
8.3	Side and Covert Channel Classification	94
8.4	Estimates of Existing Attack Bandwidths	96
8.4.1	Attack Bandwidth Analysis	97
8.5	Defending Side and Covert Channels	98
8.5.1	Hardware-Based Defenses Overview	98
8.5.2	Secure Cache Designs	100
8.5.3	Software-Based Defenses	101
8.5.4	Combining Defenses Overview	102
8.6	Side Channels as Attack Detectors	102
8.7	Side-Channel Threats Assumption	102
8.7.1	Side-Channel Free TEE Assumption	102
9	Security Verification of Processor Architectures	103
9.1	Motivation for Formal Security Verification	103
9.2	Security Verification across Different Levels of Abstraction	104
9.3	Security Verification Approaches	105
9.3.1	System Representation	106
9.3.2	Security Properties	107
9.3.3	Formal Verification	108
9.4	Discussion of Hardware-Software Security Verification Projects	109

9.5	Security Verification Assumption	111
9.5.1	Verified TCB Assumption	111
9.5.2	Verified TEE Software Assumption	111
10	Principles of Secure Processor Architecture Design	113
10.1	The Principles	113
10.1.1	Protect Off-Chip Communication and Memory	113
10.1.2	Isolate Processor State Between TEE Execution	114
10.1.3	Measure and Continuously Monitor TCB and TEE	114
10.1.4	Allow TCB Introspection	114
10.1.5	Minimize the TCB	115
10.2	Impact of Secure Design Principles on the Processor Architecture Principles	115
10.3	Limitations of the Secure Processor Assumptions	116
10.4	Pitfalls and Fallacies	118
10.5	Challenges in Secure Processor Design	121
10.6	Future Trends in Secure Processor Designs	122
10.7	Art and Science of Secure Processor Design	123
	Bibliography	125
	Online Resources	149
	Author's Biography	151

Preface

Recent years have brought increased interest in hardware security features that can be added to computer processors to protect sensitive code and data. It has been realized that new hardware security features can be used to provide, for example, means of authentication or protection of confidentiality and integrity. The hardware offers a very high level of immutability, helping to ensure that it is difficult to change the hardware security protections (unlike with software-only protections). Hardware cannot be as easily bypassed or subverted as software, as it is the ultimate lowest layer of a computer system. Finally, dedicated hardware for providing security protections can potentially offer energy efficiency and minimal impact on system performance.

Yet, adding security features in hardware has many challenges. Defining what has to be secured, and how, is often a subjective choice based on qualitative arguments—unlike the quantitative choices that computer architects are used to making. Moreover, once made, the hardware cannot be easily changed, which necessitates careful design of the security features in the first place. The secure architecture design process also requires foresight to include features and algorithms that will be suitable for many years to come. Perhaps the biggest challenges are the attacks and various information leaks that the system should protect against. Not only random errors or faults need to be considered, but the system also needs to defend against “smart” attackers who can intelligently manipulate inputs or probe the hardware to try to maximize their chances of subverting the computer system’s protections.

This book assumes readers may be at the level of a first- or second-year graduate student in computer architecture. The book is also suitable for more senior students or for practicing computer architects who are interested in starting work on the design of secure processor architectures. The book provides a chapter on security topics such as encryption, hashing, confidentiality, and integrity, to name a few—consequently a background in computer security is not required. It is the hope that this book will get computer architects excited about security and help them work on secure processor architectures.

The chapters of this book are based on research ideas developed by the author and also ideas gleaned from papers that a variety of researchers have presented in conferences such as ISCA, ASPLOS, HPCA, CCS, S&P, and Usenix Security. Information is also included about recent commercial architectures, such as Intel SGX, ARM TrustZone, and AMD memory encryption technologies. The book, however, is not meant as a manual or tutorial about any one specific security architecture. Rather, it uses past academic and industry research to derive and present the principles behind design of such secure processor architectures.

This book is divided into ten chapters. Chapter 1 focuses on motivating the need for secure processor architectures and gives an overview of the book’s organization. Chapter 2 covers

basics of computer security needed for understanding secure processor architecture designs. It can be considered an optional chapter for those already familiar with major computer security topics. Chapter 3 discusses main features of secure processor architectures, such as extending processors with new privilege levels, or breaking the traditional linear hierarchy of the privilege levels. Chapter 4 focuses on the Trusted Execution Environments which are created by the hardware and software Trusted Computing Base, and discusses various protections that secure architectures can offer to the Trusted Execution Environments. Chapter 5 introduces the Root of Trust from which most of the security features of a secure processor architecture are derived. Chapter 6 is an in-depth discussion of protections that secure architectures use to protect main memory, usually DRAM. Chapter 7 overviews security features that target designs with many processors or many processor cores. Chapter 8 gives extended review of side channel threats, processor features that contribute to existence of side channels, and ideas for eliminating various side channels. Chapter 9 is an optional chapter, which can be considered a mini survey of work on security verification of processor architectures and hardware. Chapter 10 concludes the book by presenting the five principles for secure processor architecture design, along with research challenges and future trends in secure processor designs.

After finishing this book, readers should be familiar with the five design principles for secure processor architecture design, numerous design suggestions, as well as become educated about pitfalls and fallacies that they should avoid when working on secure processor designs. Most importantly, security at the processor and hardware level is a crucial aspect of today's computers, and this book aims to educate and excite readers about this research area and its possibilities.

Jakub Szefer
October 2018

Acknowledgments

The ideas and principles derived in this book are based not only on my own research, but also on research and ideas explored over many years by numerous researchers and gleaned from their academic papers presented in top architecture and security conferences. I would like to especially acknowledge my former Ph.D. adviser, Prof. Ruby B. Lee, and others with whom I learned about, and worked on, secure processor architectures. The principles and ideas presented here reflect the hard work of many researchers and of the broader computer architecture and security communities.

I would like to thank Prof. Margaret Martonosi, the editor of the Synthesis Lectures on Computer Architecture series, and Michael B. Morgan, President and CEO of Morgan & Claypool Publishers, for their support and deadline extensions. I hope this book is a valuable addition to the series, and it was made much better through their input and encouragement. In addition, this book was improved thanks to the feedback and reviews from Margaret Martonosi, Caroline Trippel, and Chris Fletcher. Further, I would like to thank Dr. C.L. Tondo, Christine Kiilerich, and the copyeditors for helping bring this book to reality.

Work on this book was made possible in part through generous support from the National Science Foundation, through grants number 1716541, 1524680, and an NSF CAREER award number 1651945, and through support by Semiconductor Research Corporation (SRC). It was further made possible through support from Yale University.

Special thanks to my current Ph.D. students: Wenjie Xiong, Wen Wang, Shuwen Deng, and Shanquan Tian. It is a pleasure to work with them on secure processor architectures, hardware security, and other topics related to improving computer hardware security; our work forces me to constantly learn new ideas and push the boundaries on these exciting research topics.

I would like to thank my parents, Ewa and Krzysztof, for their constant encouragement, especially during my years in graduate school, and now in my academic career. Their unwavering love and support can always be counted on.

Most importantly, I would like to thank my amazing wife, Injoong, for all she does. Without her, my research, work, and this book would not be possible. She is the most loving wife and my best friend. And last, but not least, many hugs and kisses to our baby daughter, Adriana, for being the cutest and smartest baby ever! Every day is a surprise and she brings nothing but joy to me.