Security Basics for Computer Architects

Synthesis Lectures on Computer Architecture

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.

Security Basics for Computer Architects
Ruby B. Lee
2013

The Datacenter as a Computer: An Introduction to the Design of Warehouse-Scale Machines, 2nd 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 , Meeta Sharma Gupta
2013

Multithreading Architecture
Mario Nemirovsky, Dean M. Tullsen
2013

Performance Analysis and Tuning for General Purpose Graphics Processing Units (GPGPU)
Hyesoon Kim, Richard Vuduc, Sara Baghsorkhi, Jee Choi, 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 Gurumurthi, Bipin Rajendran
2011

Multi-Core Cache Hierarchies
Rajeev Balasubramonian, Norman P. Jouppi, Naveen Muralimanohar
2011

A Primer on Memory Consistency and Cache Coherence
Daniel J. Sorin, Mark D. Hill, 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, Frederic T. Chong
2011

High Performance Datacenter Networks: Architectures, Algorithms, and Opportunities
Dennis Abts, John Kim
2011

Processor Microarchitecture: An Implementation Perspective
Antonio González, Fernando Latorre, Grigorios Magklis
2010

Transactional Memory, 2nd edition
Tim Harris , James Larus , Ravi Rajwar
2010

Computer Architecture Performance Evaluation Methods
Lieven Eeckhout
2010

Introduction to Reconfigurable Supercomputing
Marco Lanzagorta, Stephen Bique, Robert Rosenberg
2009

On-Chip Networks
Natalie Enright Jerger, 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, Urs Hölzle
2009

Computer Architecture Techniques for Power-Efficiency
Stefanos Kaxiras, Margaret Martonosi
2008

Chip Multiprocessor Architecture: Techniques to Improve Throughput and Latency
Kunle Olukotun, Lance Hammond, James Laudon
2007

Transactional Memory
James R. Larus, Ravi Rajwar
2006

Quantum Computing for Computer Architects
Tzvetan S. Metodi, Frederic T. Chong
2006

Security Basics for Computer Architects
Ruby B. Lee

ISBN: 978-3-031-00614-2 print
ISBN: 978-3-031-01742-1 ebook

DOI 10.1007/978-3-031-01742-1

A Publication in the Springer series
SYNTHESIS LECTURES ON COMPUTER ARCHITECTURE
Lecture #25
Series Editor: Mark D. Hill, University of Wisconsin, Madison

Series ISSN 1935-3235 Print 1935-3243 Electronic

Security Basics for Computer Architects

Ruby B. Lee
Princeton University

SYNTHESIS LECTURES ON COMPUTER ARCHITECTURE #25

ABSTRACT

Design for security is an essential aspect of the design of future computers. However, security is not well understood by the computer architecture community. Many important security aspects have evolved over the last several decades in the cryptography, operating systems, and networking communities. This book attempts to introduce the computer architecture student, researcher, or practitioner to the basic concepts of security and threat-based design. Past work in different security communities can inform our thinking and provide a rich set of technologies for building architectural support for security into all future computers and embedded computing devices and appliances. I have tried to keep the book short, which means that many interesting topics and applications could not be included. What the book focuses on are the fundamental security concepts, across different security communities, that should be understood by any computer architect trying to design or evaluate security-aware computer architectures.

The book is also written to be accessible to a more general audience interested in the basic security technologies that can be used to improve cyber security. By understanding the concepts behind the security terminology, the interested reader would understand more clearly the frequent security breaches being reported in the news and be able to critique or even help propose effective security solutions.

KEYWORDS

computer security, trustworthy computing, hardware security, cryptography, security policies, access control, secure protocols, secure processors, confidentiality and integrity

Contents

Preface

There are certain security fundamentals that underlie the design of secure systems for computation, storage and transmission of digital information. It is essential to understand these basic concepts and learn the terminology used by the security community. They will inform our design of secure computer architectures. This book attempts to summarize for computer architects some of the most important security basics, usually taught in separate classes on cryptography, operating systems security and network security.

OUTLINE OF THE BOOK

In Chapter 1, we introduce threat-based design for computer architects, complementing the current performance-based, power-based, area-based and cost-based design approaches. We define the cornerstone security properties of Confidentiality, Integrity and Availability. We also define fundamental access control, as well as other desirable security properties. We define what we mean by a *security-aware computer*, which we also call a *trustworthy computer*. We also propose a systematic security architecture design methodology.

In Chapters 2 through 6, we introduce the computer architect to important security technology regarding security policies, access control mechanisms, cryptographic techniques and security protocols. A unique aspect of this book is that we give examples of how computer architects have used these security techniques in the design of trustworthy computers.

Chapter 2 describes security policy models for both multi-level and multi-lateral security. This helps the computer architect learn the terminology and understand how to think about security policies for protecting confidentiality or integrity. The use of security policy models enables us to focus on the basic concepts, rather than the myriad other details in real-life security policies.

Chapter 3 describes basic access control, comprising authentication and authorization mechainisms. While these mechanisms have typically been implemented by Operating Systems (OS), they may have to be implemented by trusted hypervisors or hardware, especially when the OS is compromised.

Chapters 4 and 5 provide an introduction to cryptography. This is a highly developed field that provides invaluable cryptographic primitives that the computer architect can use. We describe it as a new way of thinking where instead of restricting access (as in many of the security policy models and access control mechanisms in Chapters 2 and 3), the idea is to allow free access to cryptographically protected information, except restricting the access to the cryptographic keys that allow making sense of the encrypted material.

Chapter 4 describes symmetric-key ciphers and cryptographic hash algorithms, which can be used to facilitate protection of confidentiality and integrity, respectively, in computer systems.

Chapter 5 describes public-key cryptography, which can be used to provide longer-term digital identities. Digital signatures, Public Key Infrastructure (PKI), Certificates and Certificate Authorities (CAs) are discussed, as well as the dangers of man-in-the-middle attacks and misunderstanding public-key cryptography.

Chapter 6 presents security protocols, which are used to establish secure communications across the network, and between computers. They can also be used to describe interactions between components within a computer. Security protocols are essential aspects of a security architecture, cutting across its software, hardware and networking components. The use of strong cryptography becomes useless, if the protocols used to interact between the sender and the recipient are not secure.

Chapter 7 summarizes the topics covered, points to some interesting application areas and hardware-related security topics, and the road ahead for designing security-aware architectures.

A reader who just wants to understand the basic security concepts, but not to design a secure computer, can skip the architecture design examples. One who just wants to understand or implement simple cryptographic processing can skip Chapters 2 and 3. However, any computer architect seriously considering designing for security should read the entire book. It describes fundamental security concepts that enable us to converse with the security community and understand how to approach threat-based design.

For expediency, I have often used as examples the architectures we have designed at PALMS (Princeton Architecture Lab for Multimedia and Security, palms.ee.princeton.edu) to illustrate how the security concepts presented in this book can be used in the design of hardware-software security architectures. These examples are very familiar to me and hence easier for me to write about quickly. I also give some examples of other designs and extensive lists of references to related work in some areas. A subsequent book will discuss specific new security research topics for computer architects. The goal of this book is to condense the vast amount of security basics into a short tutorial. Hence, the topics I have chosen are fundamental ones for understanding some of the dimensions and nuances of security, and can inform new work in the design of security-aware systems.

Computer architects used to building systems must now also learn to think about how systems can be broken or exploited by attackers. We need to learn how to design proactively to thwart such malicious acts. The basic security concepts described in these chapters provide us with a rich starting set of ideas and techniques for thinking about the design of new hardware-software security architectures.

I would like to thank my teaching assistants and students in my Princeton undergraduate class, ELE/EGR 386 Cyber Security, and my graduate seminar class, ELE/COS 580 Trustworthy Computing, for their interesting inputs to my lectures and discussions. The book reflects material from some of my lectures in these classes. Many thanks go to Mark Hill who instinctively appreciated the importance of security in computer architecture, invited me several times to write a book on security, and would not take no for an answer. Mike Morgan also provided constant encouragement in getting me to finish this book. Finally, I wish to thank my dear husband, Howard, who makes life fun and supports me so lovingly, whether I am writing a book or not.