

Preface

The purpose of this book is to provide a practical approach to managing security in FPGA designs for researchers and practitioners in the electronic design automation (EDA) and FPGA communities, including corporations, industrial and government research labs, and academics. This book combines theoretical underpinnings with a practical design approach and worked examples for combating real world threats. To address the spectrum of lifecycle and operational threats against FPGA systems, a holistic view of FPGA security is presented, from formal top level specification to low level policy enforcement mechanisms, which integrates recent advances in the fields of computer security theory, languages, compilers, and hardware. The net effect is a diverse set of static and runtime techniques that, working in cooperation, facilitate the composition of robust, dependable, and trustworthy systems using commodity components.

We wish to acknowledge the many people who helped us ensure the success of our work on reconfigurable hardware security. In particular, we wish to thank Andrei Paun and Jason Smith of Louisiana Tech University for providing us with a Linux-compatible version of Grail+. We also wish to thank those who gave us comments on drafts of this book, including Marco Platzner of the University of Paderborn, and Ali Irturk and Jason Oberg of the University of California, San Diego. This research was funded in part by National Science Foundation Grant CNS-0524771 and NSF Career Grant CCF-0448654.

Monterey, CA, USA

La Jolla, CA, USA
Santa Barbara, CA, USA

Ted Huffmire
Cynthia Irvine
Thuy D. Nguyen
Timothy Levin
Ryan Kastner
Timothy Sherwood

Ted Huffmire is an assistant professor of computer science at the Naval Postgraduate School in Monterey, California. His research spans both computer security and computer architecture, focusing on hardware-oriented security and the development of policy enforcement mechanisms for application-specific devices. He has a Ph.D. in computer science from the University of California, Santa Barbara. He is a member of the IEEE and the ACM.

Cynthia Irvine is the director of the Center for Information Systems Security Studies and Research (CISR) and a professor of computer science at the Naval Postgraduate School in Monterey, California. Her research interests include high-assurance security. She has a Ph.D. in astronomy from Case Western Reserve University. She is a member of the IEEE, the ACM, and the Astronomical Society of the Pacific.

Thuy D. Nguyen is a senior researcher of computer science at the Naval Postgraduate School in Monterey, California. Her research interests include high-assurance platforms, trusted operating systems, dynamic security services, multilevel security, security evaluation, and security requirements engineering. She has a B.A. in computer science from the University of California, San Diego.

Timothy Levin is an associate research professor at the Naval Postgraduate School in Monterey, California. His research interests include design, analysis and verification of high-assurance security architectures and dynamic security policies. He has a B.S. in computer science from the University of California, Santa Cruz. He is a member of the IEEE and the ACM.

Ryan Kastner is an associate professor in the Department of Computer Science and Engineering at the University of California, San Diego. His research interests focus on many aspects of embedded computing systems, including reconfigurable architectures, digital-signal processing, and security. He has a Ph.D. in computer science from the University of California, Los Angeles.

Timothy Sherwood is an associate professor in the Department of Computer Science at the University of California, Santa Barbara. His research interests include computer architecture, specifically in the development of novel high-throughput methods by which systems can be constructed, monitored, and analyzed. He has a Ph.D. in computer science and engineering from the University of California, San Diego. He is a member of the IEEE and the ACM.

<http://www.springer.com/978-90-481-9156-7>

Handbook of FPGA Design Security

Huffmire, T.; Irvine, C.; Nguyen, T.D.; Levin, T.; Kastner,
R.; Sherwood, T.

2010, XVIII, 177 p., Hardcover

ISBN: 978-90-481-9156-7