OMB No. 7429164658510

Boundary Scan Security Enhancements For A Cryptographic

What is Boundary Scan? Boundary Scan Standard Boundary Scan Basic Tutorial EEVblog #499 - What is JTAG and Boundary Scan? Advantages and Applications of Boundary-scan Diploma Work - Boundary Scan Testing on Student Built PCB Who Uses JTAG Boundary Scan Tessent BoundaryScan - Use of Boundary Scan chain during ATPG Tessent IJTAG - Converting Boundary-Scan Language Description Files JTAG/Boundary Scan: Basics ScanWorks Boundary-Scan Test Product Demo JTAG Testing with XJTAG Boundary Scan what-is-jtag-boundary-scan.mp4 Embedded Test with JTAG - Enhancing Boundary-Scan XJDeveloper for Creating Powerful Boundary Scan Tests What is JTAG and why use it? (FULL Presentation) 12 2 DFT2 JTAG Registers
Cryptographic Hardware and Embedded Systems -- CHES 2012
Field-programmable Logic and Applications
Nanometer Design for Testability
5th International Workshop, FPL '95, Oxford, United Kingdom, August 29 - September 1, 1995. Proceedings
Programmable Logic
Computer Aided Systems Theory - EUROCAST 2009
ZigBee Wireless Networks and Transceivers
System-on-Chip Test Architectures
Specification, Implementation and Verification
EDN, Electrical Design News
Design and Deployment of Integrated Circuits in a Threatened Environment
Recommendations of the National Institute of Standards and Technology
Requirements, Test Cases, and Testing Methods
Secure and Resilient Software
Intelligent Technical Systems
An In-Depth Guide to Mobile Device Forensics
Attacks and Countermeasures
... International Workshop, FPL ..., Proceedings

Boundary Scan Security Enhancements For A Cryptographic *OMB No. 7429164658510 edited by*

MARISA ROBERTS

Cryptographic Hardware and Embedded Systems -- CHES 2012

CRC Press
Secure and Resilient Software: Requirements, Test Cases, and Testing Methods provides a comprehensive set of requirements for secure and resilient software development and operation. It supplies documented test cases for those requirements as well as best practices for testing nonfunctional requirements for improved information assurance. This resource-rich book includes: Pre-developed nonfunctional requirements that can be reused for any software development project Documented test cases that go along with the requirements and can be used to develop a Test Plan for the software Testing methods that can be applied to the test cases provided A CD with all security requirements and test cases as well as MS Word versions of the checklists, requirements, and test cases covered in the book Offering ground-level, already-developed software nonfunctional requirements and corresponding test cases and methods, this book will help to ensure that your software meets its nonfunctional requirements for security and resilience. The accompanying CD filled with helpful checklists and reusable documentation provides you with the tools needed to integrate security into the requirements analysis, design, and testing phases of your software development lifecycle. Some Praise for the Book: This book pulls together the state of the art in thinking about this important issue in a holistic way with several examples. It takes you through the entire lifecycle from conception to implementation ... . —Doug Cavit, Chief Security Strategist, Microsoft Corporation ...provides the reader with the tools necessary to jump-start and mature security within the software development lifecycle (SDLC). —Jeff Weekes, Sr. Security Architect at Terra Verde Services ... full of useful insights and practical advice from two authors who have lived

this process. What you get is a tactical application security roadmap that cuts through the noise and is immediately applicable to your projects. —Jeff Williams, Aspect Security CEO and Volunteer Chair of the OWASP Foundation

Field-programmable Logic and Applications Elsevier

This book offers readers comprehensive coverage of security policy specification using new policy languages, implementation of security policies in Systems-on-Chip (SoC) designs – current industrial practice, as well as emerging approaches to architecting SoC security policies and security policy verification. The authors focus on a promising security architecture for implementing security policies, which satisfies the goals of flexibility, verification, and upgradability from the ground up, including a plug-and-play hardware block in which all policy implementations are enclosed. Using this architecture, they discuss the ramifications of designing SoC security policies, including effects on non-functional properties (power/performance), debug, validation, and upgrade. The authors also describe a systematic approach for “hardware patching”, i.e., upgrading hardware implementations of security requirements safely, reliably, and securely in the field, meeting a critical need for diverse Internet of Things (IoT) devices. Provides comprehensive coverage of SoC security requirements, security policies, languages, and security architecture for current and emerging computing devices; Explodes myths and ambiguities in SoC security policy implementations, and provide a rigorous treatment of the subject; Demonstrates a rigorous, step-by-step approach to developing a diversity of SoC security policies; Introduces a rigorous, disciplined approach to “hardware patching”, i.e., secure technique for updating hardware functionality of computing devices in-field; Includes discussion of current and emerging approaches for security policy verification.

Nanometer Design for Testability CRC Press

This book introduces readers to various threats faced during design and fabrication by today’s integrated circuits (ICs) and systems. The authors discuss key issues, including illegal manufacturing of ICs or “IC Overproduction,” insertion of malicious circuits, referred as “Hardware Trojans”, which cause in-field chip/system malfunction, and reverse engineering and piracy of hardware intellectual property (IP). The authors provide a timely discussion of these threats, along with techniques for IC protection based on hardware obfuscation, which makes reverse-engineering an IC design infeasible for adversaries and untrusted parties with any reasonable amount of resources. This exhaustive study includes a review of the hardware obfuscation methods developed at each level of abstraction (RTL, gate, and layout) for conventional IC manufacturing, new forms of obfuscation for emerging integration strategies (split manufacturing, 2.5D ICs, and 3D ICs), and on-chip infrastructure needed for secure exchange of obfuscation keys- arguably the most critical element of hardware obfuscation.

5th International Workshop, FPL '95, Oxford, United Kingdom, August 29 - September 1, 1995. Proceedings CRC Press

In response to tremendous growth and new technologies in the semiconductor industry, this volume is organized into five, information-rich sections. Digital Design and Fabrication surveys the latest advances in computer architecture and design as well as the technologies used to manufacture and test them. Featuring contributions from leading experts, the book also includes a new section on memory and storage in addition to a new chapter on nonvolatile memory technologies. Developing advanced concepts, this sharply focused book— Describes new technologies that have become driving factors for the electronic industry Includes new information on semiconductor memory circuits, whose development best illustrates the phenomenal progress encountered by the fabrication and technology sector Contains a section dedicated to issues related to system power consumption Describes reliability and testability of computer systems Pinpoints trends and state-of-the-art advances in fabrication and CMOS technologies Describes performance evaluation measures, which are the bottom line from the user’s point of view Discusses design techniques used to create modern computer systems, including high-speed computer arithmetic and high-frequency design, timing and clocking, and PLL and DLL design

Programmable Logic Springer Science & Business Media

The consumer electronics market has never been as awash with new consumer products as it has over the last couple of years. The devices that have emerged on the scene have led to major changes in the way consumers listen to music, access the Internet, communicate, watch videos, play games, take photos, operate their automobiles—even live. Digital electronics has led to these leaps in product development, enabling easier exchange of media, cheaper and more reliable products, and convenient services. This handbook is a much-needed, comprehensive engineering guide to the dynamic world of today's digital consumer electronics. It provides complete details on key enabling technologies, standards, delivery and reception systems, products, appliances and networking systems. Each chapter follows a logical progression from a general overview of each device, to market dynamics, to the core technologies and components that make up that particular product. The book thoroughly covers all of the key digital consumer product categories: digital TV, digital audio, mobile communications devices, gaming consoles, DVD players, PCs and peripherals, display devices, digital imaging devices, web terminals and pads, PDAs and other handhelds, screenphones/videophones, telematics devices, eBooks and readers, and many other current and future products. To receive a FREE daily newsletter on displays and consumer electronics, go to: http://www.displaydaily.com/ ·Surveys crucial engineering information for every digital consumer product category, including cell phones, digital TVs, digital cameras, PDAs and many more—the only reference available to do so ·Has extremely broad market appeal to embedded systems professionals, including engineers, programmers, engineering managers, marketing and sales personnel—1,000,000+ potential readers ·Helps engineers and managers make the correct design decisions based on real-world data

Computer Aided Systems Theory - EUROCAST 2009 Conference

This book constitutes the proceedings of the 14th International Workshop on Cryptographic Hardware and Embedded Systems, CHES 2012, held in Leuven, Belgium, in September 2012. The 32 papers presented together with 1 invited talk were carefully reviewed and selected from 120 submissions. The papers are organized in the following topical sections: intrusive attacks and countermeasures; masking; improved fault attacks and side channel analysis; leakage resiliency and security analysis; physically unclonable functions; efficient implementations; lightweight cryptography; we still love RSA; and hardware implementations.

ZigBee Wireless Networks and Transceivers Springer

This book provides the foundations for understanding hardware security and trust, which have

become major concerns for national security over the past decade. Coverage includes security and trust issues in all types of electronic devices and systems such as ASICs, COTS, FPGAs, microprocessors/DSPs, and embedded systems. This serves as an invaluable reference to the state-of-the-art research that is of critical significance to the security of, and trust in, modern society's microelectronic-supported infrastructures.

System-on-Chip Test Architectures

Springer Science & Business Media
This book provides readers with a valuable reference on cyber weapons and, in particular, viruses, software and hardware Trojans. The authors discuss in detail the most dangerous computer viruses, software Trojans and spyware, models of computer Trojans affecting computers, methods of implementation and mechanisms of their interaction with an attacker — a hacker, an intruder or an intelligence agent. Coverage includes Trojans in electronic equipment such as telecommunication systems, computers, mobile communication systems, cars and even consumer electronics. The evolutionary path of development of hardware Trojans from "cabinets", "crates" and "boxes" to the microcircuits (IC) is also discussed. Readers will benefit from the detailed review of the major known types of hardware Trojans in chips, principles of their design, mechanisms of their functioning, methods of their introduction, means of camouflaging and detecting, as well as methods of protection and counteraction.
Specification, Implementation and Verification Springer Science & Business Media
Boundary-Scan, formally known as IEEE/ANSI Standard 1149.1-1990, is a collection of design rules applied principally at the Integrated Circuit (IC) level that allow software to alleviate the growing cost of designing, producing and testing digital systems. A fundamental benefit of the standard is its ability to transform extremely difficult printed circuit board testing problems that could only be attacked with ad-hoc testing methods into well-structured problems that software can easily deal with. IEEE standards, when embraced by practicing engineers, are living entities that grow and change quickly. The Boundary-Scan Handbook, Second Edition: Analog and Digital is intended to describe these standards in simple English rather than the strict and pedantic legalese encountered in the standards. The 1149.1 standard is now over eight years old and has a large infrastructure of support in the electronics industry. Today, the majority of custom ICs and programmable devices contain 1149.1. New applications for the 1149.1 protocol have been introduced, most notably the `In-System Configuration' (ISC) capability for Field Programmable Gate Arrays (FPGAs). The Boundary-Scan Handbook, Second Edition: Analog and Digital updates the information about IEEE Std. 1149.1, including the 1993 supplement that added new silicon functionality and the 1994 supplement that formalized the BSDL language definition. In addition, the new second edition presents completely new information about the newly approved 1149.4 standard often termed `Analog Boundary-Scan'. Along with this is a discussion of Analog Metrology needed to make use of 1149.1. This forms a toolset essential for testing boards and systems of the future.
EDN, Electrical Design News No Starch Press
This book is about security in embedded systems and it provides an authoritative reference to all aspects of security in system-on-chip (SoC) designs. The authors discuss issues ranging from security requirements in SoC designs, definition of architectures and design choices to enforce and validate security policies, and trade-offs and conflicts involving security, functionality, and debug requirements. Coverage also includes case studies from the "trenches" of current industrial practice in design, implementation, and validation of security-critical embedded systems. Provides an authoritative reference and summary of the current state-of-the-art in security for embedded systems, hardware IPs and SoC designs; Takes a "cross-cutting" view of security that interacts with different design and validation components such as architecture, implementation, verification, and debug, each enforcing unique trade-offs; Includes high-level overview, detailed analysis on implementation, and relevant case studies on design/verification/debug issues related to IP/SoC security.

Design and Deployment of Integrated Circuits in a Threatened Environment

Elsevier
Intelligent technical systems are networked, embedded systems incorporating real-time capacities that are able to interact with and adapt to their environments. These systems need innovative approaches in order to meet requirements like cost, size, power and memory consumption, as well as real-time compliance and security. Intelligent Technical Systems covers different levels like multimedia systems, embedded programming, middleware platforms, sensor networks and autonomous systems and applications for intelligent engineering. Each level is discussed by a set of original articles summarizing the state of the art and presenting a concrete application; they include a deep discussion of their model and explain all design decisions relevant to obtain a mature solution.
Recommendations of the National Institute of Standards and Technology Springer
ZigBee is a short-range wireless networking standard backed by such industry leaders as Motorola, Texas Instruments, Philips, Samsung, Siemens, Freescale, etc. It supports mesh networking, each node can transmit and receive data, offers high security and robustness, and is being rapidly adopted in industrial, control/monitoring, and medical applications. This book will explain the ZigBee protocol, discuss the design of ZigBee hardware, and describe how to design and implement ZigBee networks. The book has a dedicated website for the latest technical updates, ZigBee networking calculators, and additional materials. Dr. Farahani is a ZigBee system engineer for Freescale semiconductors Inc. The book comes with a dedicated website that contains additional resources and calculators: http://www.learnZigBee.com Provides a comprehensive overview of ZigBee technology and networking, from RF/physical layer considerations to application layer development Discusses ZigBee security features such as encryption Describes how ZigBee can be used in location detection applications Explores techniques for ZigBee co-existence with other wireless technologies such as 802.11 and Bluetooth The book comes with a dedicated website that contains additional resources and calculators: http://www.learnZigBee.com

Requirements, Test Cases, and Testing Methods

Springer
This book provides an overview of state-of-the-art research on "Systems and Optimization Aspects of

Smart Grid Challenges." The authors have compiled and integrated different aspects of applied systems optimization research to smart grids, and also describe some of its critical challenges and requirements. The promise of a smarter electricity grid could significantly change how consumers use and pay for their electrical power, and could fundamentally reshape the current Industry. Gaining increasing interest and acceptance, Smart Grid technologies combine power generation and delivery systems with advanced communication systems to help save energy, reduce energy costs and improve reliability. Taken together, these technologies support new approaches for load balancing and power distribution, allowing optimal runtime power routing and cost management. Such unprecedented capabilities, however, also present a set of new problems and challenges at the technical and regulatory levels that must be addressed by Industry and the Research Community.

Secure and Resilient Software Springer Science & Business Media

Test functions (fault detection, diagnosis, error correction, repair, etc.) that are applied concurrently while the system continues its intended function are defined as on-line testing. In its expanded scope, on-line testing includes the design of concurrent error checking subsystems that can be themselves self-checking, fail-safe systems that continue to function correctly even after an error occurs, reliability monitoring, and self-test and fault-tolerant designs. On-Line Testing for VLSI contains a selected set of articles that discuss many of the modern aspects of on-line testing as faced today. The contributions are largely derived from recent IEEE International On-Line Testing Workshops. Guest editors Michael Nicolaidis, Yervant Zorian and Dhiraj Pradhan organized the articles into six chapters. In the first chapter the editors introduce a large number of approaches with an expanded bibliography in which some references date back to the sixties. On-Line Testing for VLSI is an edited volume of original research comprising invited contributions by leading researchers.

Intelligent Technical Systems

Computer Aided Systems Theory - EUROCAST 200912th International Conference, Las Palmas de Gran Canaria, Spain, February 15-20, 2009, Revised Selected Papers

The Hardware Hacking Handbook takes you deep inside embedded devices to show how different kinds of attacks work, then guides you through each hack on real hardware. Embedded devices are chip-size microcomputers small enough to be included in the structure of the object they control, and they're everywhere—in phones, cars, credit cards, laptops, medical equipment, even critical infrastructure. This means understanding their security is critical. The Hardware Hacking Handbook takes you deep inside different types of embedded systems, revealing the designs, components, security limits, and reverse-engineering challenges you need to know for executing effective hardware attacks. Written with wit and infused with hands-on lab experiments, this handbook puts you in the role of an attacker interested in breaking security to do good. Starting with a crash course on the architecture of embedded devices, threat modeling, and attack trees, you'll go on to explore hardware interfaces, ports and communication protocols, electrical signaling, tips for analyzing firmware images, and more. Along the way, you'll use a home testing lab to perform fault-injection, side-channel (SCA), and simple and differential power analysis (SPA/DPA) attacks on a variety of real devices, such as a crypto wallet. The authors also share insights into real-life attacks on embedded systems, including Sony's PlayStation 3, the Xbox 360, and Philips Hue lights, and provide an appendix of the equipment needed for your hardware hacking lab – like a multimeter and an oscilloscope – with options for every type of budget. You'll learn: • How to model security threats, using attacker profiles, assets, objectives, and countermeasures • Electrical basics that will help you understand communication interfaces, signaling, and measurement • How to identify injection points for executing clock, voltage, electromagnetic, laser, and body-biasing fault attacks, as well as practical injection tips • How to use timing and power analysis attacks to extract passwords and cryptographic keys • Techniques for leveling up both simple and differential power analysis, from practical measurement tips to filtering, processing, and visualization Whether you're an industry engineer tasked with understanding these attacks, a student starting out in the field, or an electronics hobbyist curious about replicating existing work, The Hardware Hacking Handbook is an indispensable resource – one you'll always want to have onhand.

An In-Depth Guide to Mobile Device Forensics

CRC Press

In the second edition of this very successful book, Tony Sammes and Brian Jenkinson show how the contents of computer systems can be recovered, even when hidden or subverted by criminals. Equally important, they demonstrate how to insure that computer evidence is admissible in court. Updated to meet ACPO 2003 guidelines, Forensic Computing: A Practitioner's Guide offers: methods for recovering evidence information from computer systems; principles of password protection and data encryption; evaluation procedures used in circumventing a system's internal security safeguards, and full search and seizure protocols for experts and police officers.

Attacks and Countermeasures Springer

InfoWorld is targeted to Senior IT professionals. Content is segmented into Channels and Topic Centers. InfoWorld also celebrates people, companies, and projects.

... International Workshop, FPL ..., Proceedings Morgan Kaufmann

In two editions spanning more than a decade, The Electrical Engineering Handbook stands as the definitive reference to the multidisciplinary field of electrical engineering. Our knowledge continues to grow, and so does the Handbook. For the third edition, it has grown into a set of six books carefully focused on specialized areas or fields of study. Each one represents a concise yet definitive collection of key concepts, models, and equations in its respective domain, thoughtfully gathered for convenient access. Combined, they constitute the most comprehensive, authoritative resource available. Circuits, Signals, and Speech and Image Processing presents all of the basic information related to electric circuits and components, analysis of circuits, the use of the Laplace transform, as well as signal, speech, and image processing using filters and algorithms. It also examines emerging areas such as text to speech synthesis, real-time processing, and embedded signal processing. Electronics, Power Electronics, Optoelectronics, Microwaves, Electromagnetics, and Radar delves into the fields of electronics, integrated circuits, power electronics, optoelectronics, electromagnetics, light waves, and radar, supplying all of the basic information required for a deep understanding of each area. It also devotes a section to electrical effects and devices and explores the emerging fields of microlithography and power electronics. Sensors, Nanoscience, Biomedical

Engineering, and Instruments provides thorough coverage of sensors, materials and nanoscience, instruments and measurements, and biomedical systems and devices, including all of the basic information required to thoroughly understand each area. It explores the emerging fields of sensors, nanotechnologies, and biological effects. Broadcasting and Optical Communication Technology explores communications, information theory, and devices, covering all of the basic information needed for a thorough understanding of these areas. It also examines the emerging areas of adaptive estimation and optical communication. Computers, Software Engineering, and Digital Devices examines digital and logical devices, displays, testing, software, and computers, presenting the fundamental concepts needed to ensure a thorough understanding of each field. It treats the emerging fields of programmable logic, hardware description languages, and parallel computing in detail. Systems, Controls, Embedded Systems, Energy, and Machines explores in detail the fields of energy devices, machines, and systems as well as control systems. It provides all of the fundamental concepts needed for thorough, in-depth understanding of each area and devotes special attention to the emerging area of embedded systems. Encompassing the work of the world's foremost experts in their respective specialties, The Electrical Engineering Handbook, Third Edition remains the most convenient, reliable source of information available. This edition features the latest developments, the broadest scope of coverage, and new material on nanotechnologies, fuel cells, embedded systems, and biometrics. The engineering community has relied on the Handbook for more than twelve years, and it will continue to be a platform to launch the next wave of advancements. The Handbook's latest incarnation features a protective slipcase, which helps you stay organized without overwhelming your bookshelf. It is an attractive addition to any collection, and will help keep each volume of the Handbook as fresh as your latest research.

Fundamentals of IP and SoC Security "O'Reilly Media, Inc."

Modern electronics testing has a legacy of more than 40 years. The introduction of new technologies, especially nanometer technologies with 90nm or smaller geometry, has allowed the semiconductor industry to keep pace with the increased performance-capacity demands from consumers. As a result, semiconductor test costs have been growing steadily and typically amount to 40% of today's overall product cost. This book is a comprehensive guide to new VLSI Testing and Design-for-Testability techniques that will allow students, researchers, DFT practitioners, and VLSI designers to master quickly System-on-Chip Test architectures, for test debug and diagnosis of digital, memory, and analog/mixed-signal designs. Emphasizes VLSI Test principles and Design for Testability architectures, with numerous illustrations/examples. Most up-to-date coverage available, including Fault Tolerance, Low-Power Testing, Defect and Error Tolerance, Network-on-Chip (NOC) Testing, Software-Based Self-Testing, FPGA Testing, MEMS Testing, and System-In-Package (SIP) Testing, which are not yet available in any testing book. Covers the entire spectrum of VLSI testing and DFT architectures, from digital and analog, to memory circuits, and fault diagnosis and self-repair from digital to memory circuits. Discusses future nanotechnology test trends and challenges facing the nanometer design era; promising nanotechnology test techniques, including Quantum-Dots, Cellular Automata, Carbon-Nanotubes, and Hybrid Semiconductor/Nanowire/Molecular Computing. Practical problems at the end of each chapter for students.

Electronic Products Magazine Springer Nature

This book contains extended and revised versions of the best papers presented at the 21st IFIP WG 10.5/IEEE International Conference on Very Large Scale Integration, VLSI-SoC 2013, held in Istanbul, Turkey, in October 2013. The 11 papers included in the book were carefully reviewed and selected from the 48 full papers presented at the conference. An extended version of a previously unpublished high-quality paper from VLSI-SoC 2012 is also included. The papers cover a wide range of topics in VLSI technology and advanced research. They address the current trend toward increasing chip integration and technology process advancements bringing about stimulating new challenges both at the physical and system-design levels, as well as in the test of these systems.

Related with Boundary Scan Security Enhancements For A Cryptographic:
© Boundary Scan Security Enhancements For A Cryptographic Grim Dawn Class Guide
© Boundary Scan Security Enhancements For A Cryptographic Grounded Raw Science Farm
© Boundary Scan Security Enhancements For A Cryptographic Grounding Art Therapy Activities