Boundary Scan Security Enhancements For A Cryptographic

As recognized, adventure as competently as experience about lesson, amusement, as skillfully as understanding can be gotten by just checking out a ebook **Boundary Scan Security Enhancements For A Cryptographic** along with it is not directly done, you could understand even more in relation to this life, concerning the world.

We present you this proper as with ease as simple showing off to acquire those all. We present Boundary Scan Security Enhancements For A Cryptographic and numerous books collections from fictions to scientific research in any way. along with them is this Boundary Scan Security Enhancements For A Cryptographic that can be your partner.

AIX V6 Advanced Security Features Introduction and Configuration - Chris Almond 2013-08-26

AIX Version 6.1 provides many significant new security technologies and security enhancements. The purpose of this IBM Redbooks publication is to highlight and explain the security features at the conceptual level, as well as provide practical examples of how they may be implemented. Some features are extensions of features made available in prior AIX releases, and some are new features introduced with AIX V6. Major new security enhancements will be introduced with AIX V6 in 2007: - Trusted AIX (Multilevel Security) - Role Based Access Control (RBAC) - Encrypted File System - Trusted Execution - AIX Security Expert Enhancements This IBM Redbooks publication will provide a technical introduction to these new enhancements. The topics are both broad and very complex. This book will serve as an initial effort in describing all of the enhancements together in a single volume to the security/system hardening oriented audience.

Computer Aided Systems Theory - EUROCAST 2009 - Roberto Moreno Díaz 2009-09-30

The concept of CAST as Computer Aided Systems Theory was introduced by F. Pichler in the late 1980s to refer to computer theoretical and practical developments as tools for solving problems in system science. It was thought of as the third component (the other two being CAD and CAM) required to complete the path from computer and systems sciences to practical developments in science and engineering. Franz Pichler, of the University of Linz, organized the first CAST workshop in April 1988, which demonstrated the acceptance of the concepts by the scientific and technical community. Next, the University of Las Palmas de Gran Canaria joined the University of Linz to organize the first international meeting on CAST (Las Palmas, February 1989) under the name EUROCAST'89. This proved to be a very successful gathering of systems theorists, computer scientists and engineers from most European countries, North America and Japan. It was agreed that EUROCAST international conferences would be organized every two years, alternating between Las Palmas de Gran Canaria and a continental European location. From 2001 the conference has been held exclusively in Las Palmas. Thus, successive EUROCAST meetings took place in Krems (1991), Las Palmas (1993), In- bruck (1995), Las Palmas (1997), Vienna (1999), Las Palmas (2001), Las Palmas (2003) Las Palmas (2005) and Las Palmas (2007), in addition to an extra-European CAST c- ference in Ottawa in 1994.

Protocols for Secure Electronic Commerce - Mostafa Hashem Sherif 2003-11-24

The continued growth of e-commerce mandates the emergence of new technical standards and methods that will securely integrate online activities with pre-existing infrastructures, laws and processes. Protocols for Secure Electronic Commerce, Second Edition addresses the security portion of this challenge. It is a full compendium of the protocols for securing online commerce and payments, serving as an invaluable resource for students and professionals in the fields of computer science and engineering, IT security, and financial and banking technology. The initial sections provide a broad overview of electronic commerce, money, payment systems, and business-to-business commerce, followed by an examination of well-known protocols (SSL, TLS, WTLS, and SET). The book also explores encryption algorithms and methods, EDI, micropayment, and multiple aspects of digital money. Like its predecessor, this edition is a general analysis that provides many references to more technical resources. It delivers extensive revisions of previous chapters, along with new chapters on electronic commerce in society, new e-commerce systems, and the security of integrated circuit cards.

Hardware Protection through Obfuscation - Domenic Forte 2017-01-02

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.

1998 5th International Conference on Solid-State and Integrated Circuit Technology - Min Zhang 1998

International Test Conference, 1993 - 1993

Annotation Proceedings of the 24th International Test Conference held in Baltimore, October 1993--the premier conference for the testing of electronic devices, assemblies, and systems, including design for testability and diagnostics. This year's leading edge topics are mixed-signal testing, multichip modules, systems test, automatic synthesis of test structures in design, boundary scan, and Iddq. Core topics represented included ATPG, modeling, test equipment hardware, delay fault testing, software testing, DFT, applied BIST, board testing, memory and microprocessor testing, test economics, and test quality and reliability. Annotation copyright by Book News, Inc., Portland, OR.

Effective Model-Based Systems Engineering - John M. Borky 2018-09-08

This textbook presents a proven, mature Model-Based Systems Engineering (MBSE) methodology that has delivered success in a wide range of system and enterprise programs. The authors introduce MBSE as the state of the practice in the vital Systems Engineering discipline that manages complexity and integrates technologies and design approaches to achieve effective, affordable, and balanced system solutions to the needs of a customer organization and its personnel. The book begins with a summary of the background and nature of MBSE. It summarizes the theory behind Object-Oriented Design applied to complex system architectures. It then walks through the phases of the MBSE methodology, using system examples to illustrate key points. Subsequent chapters broaden the application of MBSE in Service-Oriented Architectures (SOA), real-time systems, cybersecurity, networked enterprises, system simulations, and prototyping. The vital subject of system and architecture governance completes the discussion. The book features exercises at the end of each chapter intended to help readers/students focus on key points, as well as extensive appendices

that furnish additional detail in particular areas. The self-contained text is ideal for students in a range of courses in systems architecture and MBSE as well as for practitioners seeking a highly practical presentation of MBSE principles and techniques.

Hardware Security and Trust - Nicolas Sklavos 2017-01-11

This book provides a comprehensive introduction to hardware security, from specification to implementation. Applications discussed include embedded systems ranging from small RFID tags to satellites orbiting the earth. The authors describe a design and synthesis flow, which will transform a given circuit into a secure design incorporating counter-measures against fault attacks. In order to address the conflict between testability and security, the authors describe innovative design-for-testability (DFT) computer-aided design (CAD) tools that support security challenges, engineered for compliance with existing, commercial tools. Secure protocols are discussed, which protect access to necessary test infrastructures and enable the design of secure access controllers.

Federal Cloud Computing - Matthew Metheny 2017-01-05

Federal Cloud Computing: The Definitive Guide for Cloud Service Providers, Second Edition offers an in-depth look at topics surrounding federal cloud computing within the federal government, including the Federal Cloud Computing Strategy, Cloud Computing Standards, Security and Privacy, and Security Automation. You will learn the basics of the NIST risk management framework (RMF) with a specific focus on cloud computing environments, all aspects of the Federal Risk and Authorization Management Program (FedRAMP) process, and steps for cost-effectively implementing the Assessment and Authorization (A&A) process, as well as strategies for implementing Continuous Monitoring, enabling the Cloud Service Provider to address the FedRAMP requirement on an ongoing basis. This updated edition will cover the latest changes to FedRAMP program, including clarifying guidance on the paths for Cloud Service Providers to achieve FedRAMP compliance, an expanded discussion of the new FedRAMP Security Control, which is based on the NIST SP 800-53 Revision 4, and maintaining FedRAMP compliance through Continuous Monitoring. Further, a new chapter has been added on the FedRAMP requirements for Vulnerability Scanning and Penetration Testing. Provides a common understanding of the federal requirements as they apply to cloud computing Offers a targeted and cost-effective approach for applying the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) Features both technical and non-technical perspectives of the Federal Assessment and Authorization (A&A) process that speaks across the organization

For the Record - National Research Council 1997-07-09

When you visit the doctor, information about you may be recorded in an office computer. Your tests may be sent to a laboratory or consulting physician. Relevant information may be transmitted to your health insurer or pharmacy. Your data may be collected by the state government or by an organization that accredits health care or studies medical costs. By making information more readily available to those who need it, greater use of computerized health information can help improve the quality of health care and reduce its costs. Yet health care organizations must find ways to ensure that electronic health information is not improperly divulged. Patient privacy has been an issue since the oath of Hippocrates first called on physicians to "keep silence" on patient matters, and with highly sensitive dataâ€"genetic information, HIV test results, psychiatric recordsâ€"entering patient records, concerns over privacy and security are growing. For the Record responds to the health care industry's need for greater guidance in protecting health information that increasingly flows through the national information infrastructureâ€"from patient to provider, payer, analyst, employer, government agency, medical product manufacturer, and beyond. This book makes practical detailed recommendations for technical and organizational solutions and national-level initiatives. For the Record describes two major types of privacy and security concerns that stem from the availability of health information in electronic form: the increased potential for inappropriate release of information held by individual organizations (whether by those with access to computerized records or those who break into them) and systemic concerns derived

from open and widespread sharing of data among various parties. The committee reports on the technological and organizational aspects of security management, including basic principles of security; the effectiveness of technologies for user authentication, access control, and encryption; obstacles and incentives in the adoption of new technologies; and mechanisms for training, monitoring, and enforcement. For the Record reviews the growing interest in electronic medical records; the increasing value of health information to providers, payers, researchers, and administrators; and the current legal and regulatory environment for protecting health data. This information is of immediate interest to policymakers, health policy researchers, patient advocates, professionals in health data management, and other stakeholders.

Field-Programmable Logic and Applications - Peter Y.K. Cheung 2003-08-27

This book constitutes the refereed proceedings of the 13th International Conference on Field-Programmable Logic and Applications, FPL 2003, held in Lisbon, Portugal in September 2003. The 90 revised full papers and 56 revised poster papers presented were carefully reviewed and selected from 216 submissions. The papers are organized in topical sections on technologies and trends, communications applications, high level design tools, reconfigurable architecture, cryptographic applications, multi-context FPGAs, low-power issues, run-time reconfiguration, compilation tools, asynchronous techniques, bio-related applications, codesign, reconfigurable fabrics, image processing applications, SAT techniques, application-specific architectures, DSP applications, dynamic reconfiguration, SoC architectures, emulation, cache design, arithmetic, bio-inspired design, SoC design, cellular applications, fault analysis, and network applications.

VLSI-SoC: At the Crossroads of Emerging Trends - Alex Orailoglu 2015-09-25

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.

The Electrical Engineering Handbook - Six Volume Set - Richard C. Dorf 2018-12-14

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.

Framework for Designing Cryptographic Key Management Systems - Elaine Barker 2011-05

This Framework was initiated as a part of the NIST Cryptographic Key Management Workshop. The goal was to define and develop technologies and standards that provide cost-effective security to cryptographic keys that themselves are used to protect computing and information processing applications. A Framework is a description of the components (i.e., building blocks) that can be combined or used in various ways to create a ¿system¿ (e.g., a group of objects working together to perform a vital function). This Framework identifies and discusses the components of a cryptographic key management system (CKMS) and provides requirements for CKMS design specifications conforming to this Framework. Glossary of terms. Illus. A print on demand pub.

Real-Time UML Workshop for Embedded Systems - Bruce Powel Douglass 2014-02-05

Written as a workbook with a set of guided exercises that teach by example, this book gives a practical, hands-on guide to using UML to design and implement embedded and real-time systems. A review of the basics of UML and the Harmony process for embedded software development: two on-going case examples to teach the concepts, a small-scale traffic light control system and a large scale unmanned air vehicle show the applications of UML to the specification, analysis and design of embedded and real-time systems in general. A building block approach: a series of progressive worked exercises with step-by-step explanations of the complete solution, clearly demonstrating how to convert concepts into actual designs. A walk through of the phases of an incremental spiral process: posing the problems and the solutions for requirements analysis, object analysis, architectural design, mechanistic design, and detailed design.

The Hardware Hacking Handbook - Jasper van Woudenberg 2021-12-21

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.

The Test Access Port and Boundary-scan Architecture - Colin M. Maunder 1991

Applied Cryptography and Network Security Workshops - Jianying Zhou 2021-07-21

This book constitutes the proceedings of the satellite workshops held around the 19th International Conference on Applied Cryptography and Network Security, ACNS 2021, held in Kamakura, Japan, in June 2021. The 26 papers presented in this volume were carefully reviewed and selected from 49 submissions. They stem from the following workshops: AIBlock 2021: Third International Workshop on Application Intelligence and Blockchain Security AIHWS 2021: Second International Workshop on Artificial Intelligence in Hardware Security AIoTS 2021: Third International Workshop on Artificial Intelligence and Industrial IoT Security CIMSS 2021: First International Workshop on Critical Infrastructure and Manufacturing System Security Cloud S&P 2021: Third International Workshop on Cloud Security and Privacy SCI 2021: Second International Workshop on Secure Cryptographic Implementation SecMT 2021: Second International Workshop on Security in Mobile Technologies SiMLA 2021; Third International Workshop on Security in Machine Learning and its Applications Due to the Corona pandemic the workshop was held as a virtual event.

Secure and Resilient Software - Mark S. Merkow 2011-11-10

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

System-on-Chip Test Architectures - Laung-Terng Wang 2010-07-28
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.

Computer Security - William Stallings 2012
Computer Security: Principles and Practice, 2e, is ideal for courses in Computer/Network Security. In recent years, the need for education in computer security and related topics has grown dramatically – and is essential for anyone studying Computer Science or Computer Engineering. This is the only text available to provide integrated, comprehensive, up-to-date coverage of the broad range of topics in this subject. In addition to an extensive pedagogical program, the book provides unparalleled support for both research and modeling projects, giving students a broader perspective. The Text and Academic Authors Association named Computer Security: Principles and Practice, 1e, the winner of the Textbook Excellence Award for the best Computer Science textbook of 2008.

High Performance Browser Networking - Ilya Grigorik 2013-09-11
How prepared are you to build fast and efficient web applications? This eloquent book provides what every web developer should know about the network, from fundamental limitations that affect performance to major innovations for building even more powerful browser applications—including HTTP 2.0 and XHR improvements, Server-Sent Events (SSE), WebSocket, and WebRTC. Author Ilya Grigorik, a web performance engineer at Google, demonstrates performance optimization best practices for TCP, UDP, and TLS protocols, and explains unique wireless and mobile network optimization requirements. You'll then dive into performance characteristics of technologies such as HTTP 2.0, client-side network scripting with XHR, real-time streaming with SSE and WebSocket, and P2P communication with WebRTC. Deliver superlative TCP, UDP, and TLS performance Speed up network performance over 3G/4G mobile networks Develop fast and energy-efficient mobile applications Address bottlenecks in HTTP 1.x and other browser protocols Plan for and deliver the best HTTP 2.0 performance Enable efficient real-time streaming in the browser Create efficient peer-

to-peer videoconferencing and low-latency applications with real-time WebRTC transports

Glossary of Key Information Security Terms - Richard Kissel 2011-05
This glossary provides a central resource of definitions most commonly used in Nat. Institute of Standards and Technology (NIST) information security publications and in the Committee for National Security Systems (CNSS) information assurance publications. Each entry in the glossary points to one or more source NIST publications, and/or CNSSI-4009, and/or supplemental sources where appropriate. This is a print on demand edition of an important, hard-to-find publication.

Fundamentals of IP and SoC Security - Swarup Bhunia 2017-01-24
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.

Cryptographic Hardware and Embedded Systems -- CHES 2012 - Emmanuel Prouff 2012-09-05
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.

Viruses, Hardware and Software Trojans - Anatoly Belous 2020-06-27
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.

Guidelines on Cell Phone and PDA Security - Wayne Jansen 2009-08
Cell phones and Personal Digital Assistants (PDAs) have become indispensable tools for today¿s highly mobile workforce. Small and relatively inexpensive, these devices can be used not only for voice calls, simple text messages, and Personal Information Management (PIM), but also for many functions done at a desktop computer. While these devices provide productivity benefits, they also pose new risks. This document is intended to assist organizations in securing cell phones and PDAs. More specifically, this document describes in detail the threats faced by organizations that employ handheld devices and the measures that can be taken to counter those threats.

Introduction to Hardware Security and Trust - Mohammad Tehranipoor 2011-09-22
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.

Signals - 1994

Business Week - 2002

CD-ROMs in Print - 2003

PC Mag - 1999-11-02

PCMag.com is a leading authority on technology, delivering Labs-based, independent reviews of the latest products and services. Our expert industry analysis and practical solutions help you make better buying decisions and get more from technology.

Security Policy in System-on-Chip Designs - Sandip Ray 2018-10-09

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.

Cyber Security Cryptography and Machine Learning - Shlomi Dolev 2020-06-25

This book constitutes the refereed proceedings of the Fourth International Symposium on Cyber Security Cryptography and Machine Learning, CSCML 2020, held in Be'er Sheva, Israel, in July 2020. The 12 full and 4 short papers presented in this volume were carefully reviewed and selected from 38 submissions. They deal with the theory, design, analysis, implementation, or application of cyber security, cryptography and machine learning systems and networks, and conceptually innovative topics in these research areas.

Publications of the National Institute of Standards and Technology ... Catalog - National Institute of Standards and Technology (U.S.) 1991

IBM Systems Journal - International Business Machines Corporation 1991

SOA Security - Ramarao Kanneganti 2007-12-23

SOA is one of the latest technologies enterprises are using to tame their software costs - in development, deployment, and management. SOA makes integration easy, helping enterprises not only better utilize their existing investments in applications and infrastructure, but also open up new business opportunities. However, one of the big stumbling blocks in executing SOA is security. This book addresses Security in SOA with detailed examples illustrating the theory, industry standards and best practices. It is true that security is important in any system. SOA brings

in additional security concerns as well rising out of the very openness that makes it attractive. If we apply security principles blindly, we shut ourselves of the benefits of SOA. Therefore, we need to understand which security models and techniques are right for SOA. This book provides such an understanding. Usually, security is seen as an esoteric topic that is better left to experts. While it is true that security requires expert attention, everybody, including software developers, designers, architects, IT administrators and managers need to do tasks that require very good understanding of security topics. Fortunately, traditional security techniques have been around long enough for people to understand and apply them in practice. This, however, is not the case with SOA Security. Anyone seeking to implement SOA Security is today forced to dig through a maze of inter-dependent specifications and API docs that assume a lot of prior experience on the part of readers. Getting started on a project is hence proving to be a huge challenge to practitioners. This book seeks to change that. It provides bottom-up understanding of security techniques appropriate for use in SOA without assuming any prior familiarity with security topics on the part of the reader. Unlike most other books about SOA that merely describe the standards, this book helps you get started immediately by walking you through sample code that illustrates how real life problems can be solved using the techniques and best practices described in standards. Whereas standards discuss all possible variations of each security technique, this book focusses on the 20% of variations that are used 80% of the time. This keeps the material covered in the book simple as well as self-sufficient for all readers except the most advanced. Purchase of the print book comes with an offer of a free PDF, ePub, and Kindle eBook from Manning. Also available is all code from the book.

Proceedings - 1998

Digital Design and Fabrication - Vojin G. Oklobdzija 2017-12-19

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

ZigBee Wireless Networks and Transceivers - Shahin Farahani 2011-04-08

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