

developers and customers, this book explains the key tasks in multithreading and how to accomplish them with TBB in a portable and robust manner. With plenty of examples and full reference material, the book lays out common patterns of uses, reveals the gotchas in TBB, and gives important guidelines for choosing among alternatives in order to get the best performance. You'll learn how Intel Threading Building Blocks: Enables you to specify tasks instead of threads for better portability, easier programming, more understandable source code, and better performance and scalability in general Focuses on the goal of parallelizing computationally intensive work to deliver high-level solutions Is compatible with other threading packages, and doesn't force you to pick one package for your entire program Emphasizes scalable, data-parallel programming, which allows program performance to increase as you add processors Relies on generic programming, which enables you to write the best possible algorithms with the fewest constraints Any C++ programmer who wants to write an application to run on a multi-core system will benefit from this book. TBB is also very approachable for a C programmer or a C++ programmer without much experience with templates. Best of all, you don't need experience with parallel programming or multi-core processors to use this book.

Communications represent a strategic sector for privacy protection and for personal, company, national and international security. The interception, damage or lost of information during communication can generate material and non material economic damages from both a personal and collective point of view. The purpose of this book is to give the reader information relating to all aspects of communications security, beginning at the base ideas and building to reach the most advanced and updated concepts. The book will be of interest to integrated system designers, telecommunication designers, system engineers, system analysts, security managers, technicians, intelligence personnel, security personnel, police, army, private investigators, scientists, graduate and postgraduate students and anyone that needs to communicate in a secure way.

Learn the Root Causes of Software Vulnerabilities and How to Avoid Them Commonly exploited software vulnerabilities are usually caused by avoidable software defects. Having analyzed tens of thousands of vulnerability reports since 1988, CERT has determined that a relatively small number of root causes account for most of the vulnerabilities. Secure Coding in C and C++, Second Edition, identifies and explains these root causes and shows the steps that can be taken to prevent exploitation. Moreover, this book encourages programmers to adopt security best practices and to develop a security mindset that can help protect software from tomorrow's attacks, not just today's. Drawing on the CERT's reports and conclusions, Robert C. Seacord systematically identifies the program errors most likely to lead to security breaches, shows how they can be exploited, reviews the potential consequences, and presents secure alternatives. Coverage includes technical detail on how to Improve the overall security of any C or C++ application Thwart buffer overflows, stack-smashing, and return-oriented programming attacks that exploit insecure string manipulation logic Avoid vulnerabilities and security flaws resulting from the incorrect use of dynamic memory management functions Eliminate integer-related problems resulting from signed integer overflows, unsigned integer wrapping, and truncation errors Perform secure I/O, avoiding file system vulnerabilities Correctly use formatted output functions without introducing format-string vulnerabilities Avoid race conditions and other exploitable vulnerabilities while developing concurrent code The second edition features Updates for C11 and C++11 Significant revisions to chapters on strings, dynamic memory management, and integer security A new chapter on concurrency Access to the online secure coding course offered through Carnegie Mellon's Open Learning Initiative (OLI) Secure Coding in C and C++, Second Edition, presents hundreds of examples of secure code, insecure code, and exploits, implemented for Windows and Linux. If you're responsible for creating secure C or C++ software—or for keeping it safe—no other book offers you this much detailed, expert assistance.

“At Cisco, we have adopted the CERT C Coding Standard as the internal secure coding standard for all C developers. It is a core component of our secure development lifecycle. The coding standard described in this book breaks down complex software security topics into easy-to-follow rules with excellent real-world examples. It is an essential reference for any developer who wishes to write secure and resilient software in C and C++.” —Edward D. Paradise, vice president, engineering, threat response, intelligence, and development, Cisco Systems Secure programming in C can be more difficult than even many experienced programmers realize. To help programmers write more secure code, The CERT® C Coding Standard, Second Edition, fully documents the second official release of the CERT standard for secure coding in C. The rules laid forth in this new edition will help ensure that programmers' code fully complies with the new C11 standard; it also addresses earlier versions, including C99. The new standard itemizes those coding errors that are the root causes of current software vulnerabilities in C, prioritizing them by severity, likelihood of exploitation, and remediation costs. Each of the text's 98 guidelines includes examples of insecure code as well as secure, C11-conforming, alternative implementations. If uniformly applied, these guidelines will eliminate critical coding errors that lead to buffer overflows, format-string vulnerabilities, integer overflow, and other common vulnerabilities. This book reflects numerous experts' contributions to the open development and review of the rules and recommendations that comprise this standard. Coverage includes Preprocessor Declarations and Initialization Expressions Integers Floating Point Arrays Characters and Strings Memory Management Input/Output Environment Signals Error Handling Concurrency Miscellaneous Issues C?C++????

Language and food are universal to humankind. Language accomplishes more than a pure exchange of information, and food caters for more than mere subsistence. Both represent crucial sites for socialization, identity construction, and the everyday fabrication and perception of the world as a meaningful, orderly place. This volume on Culinary Linguistics contains an introduction to the study of food and an extensive overview of the literature focusing on its role in interplay with language. It is the only publication fathoming the field of food and food-related studies from a linguistic perspective. The research articles assembled here encompass a number of linguistic fields, ranging from historical and ethnographic approaches to literary studies, the teaching of English as a foreign language, psycholinguistics, and the study of computer-mediated communication,

password protection, single sign-on, and more Discusses operating system integrity, hardware security features, and memory Covers Unix security, Windows security, database security, network security, web security, and software security Packed with in-depth coverage, this resource spares no details when it comes to the critical topic of computer security.

????????????????,????????????????????,?????????HTML & CSS????????????????????,????????????????????????????????,????????????????????????????

Instrument Engineers' Handbook – Volume 3: Process Software and Digital Networks, Fourth Edition is the latest addition to an enduring collection that industrial automation (AT) professionals often refer to as the "bible." First published in 1970, the entire handbook is approximately 5,000 pages, designed as standalone volumes that cover the measurement (Volume 1), control (Volume 2), and software (Volume 3) aspects of automation. This fourth edition of the third volume provides an in-depth, state-of-the-art review of control software packages used in plant optimization, control, maintenance, and safety. Each updated volume of this renowned reference requires about ten years to prepare, so revised installments have been issued every decade, taking into account the numerous developments that occur from one publication to the next. Assessing the rapid evolution of automation and optimization in control systems used in all types of industrial plants, this book details the wired/wireless communications and software used. This includes the ever-increasing number of applications for intelligent instruments, enhanced networks, Internet use, virtual private networks, and integration of control systems with the main networks used by management, all of which operate in a linked global environment. Topics covered include: Advances in new displays, which help operators to more quickly assess and respond to plant conditions Software and networks that help monitor, control, and optimize industrial processes, to determine the efficiency, energy consumption, and profitability of operations Strategies to counteract changes in market conditions and energy and raw material costs Techniques to fortify the safety of plant operations and the security of digital communications systems This volume explores why the holistic approach to integrating process and enterprise networks is convenient and efficient, despite associated problems involving cyber and local network security, energy conservation, and other issues. It shows how firewalls must separate the business (IT) and the operation (automation technology, or AT) domains to guarantee the safe function of all industrial plants. This book illustrates how these concerns must be addressed using effective technical solutions and proper management policies and practices. Reinforcing the fact that all industrial control systems are, in general, critically interdependent, this handbook provides a wide range of software application examples from industries including: automotive, mining, renewable energy, steel, dairy, pharmaceutical, mineral processing, oil, gas, electric power, utility, and nuclear power.

"What makes this book so important is that it reflects the experiences of two of the industry's most experienced hands at getting real-world engineers to understand just what they're being asked for when they're asked to write secure code. The book reflects Michael Howard's and David LeBlanc's experience in the trenches working with developers years after code was long since shipped, informing them of problems." --From the Foreword by Dan Kaminsky, Director of Penetration Testing, IOActive Eradicate the Most Notorious Insecure Designs and Coding Vulnerabilities Fully updated to cover the latest security issues, 24 Deadly Sins of Software Security reveals the most common design and coding errors and explains how to fix each one-or better yet, avoid them from the start. Michael Howard and David LeBlanc, who teach Microsoft employees and the world how to secure code, have partnered again with John Viega, who uncovered the original 19 deadly programming sins. They have completely revised the book to address the most recent vulnerabilities and have added five brand-new sins. This practical guide covers all platforms, languages, and types of applications. Eliminate these security flaws from your code: SQL injection Web server- and client-related vulnerabilities Use of magic URLs, predictable cookies, and hidden form fields Buffer overruns Format string problems Integer overflows C++ catastrophes Insecure exception handling Command injection Failure to handle errors Information leakage Race conditions Poor usability Not updating easily Executing code with too much privilege Failure to protect stored data Insecure mobile code Use of weak password-based systems Weak random numbers Using cryptography incorrectly Failing to protect network traffic Improper use of PKI Trusting network name resolution

Secure Programming Cookbook for C and C++

Secure Programming Cookbook for C and C++ is an important new resource for developers serious about writing secure code. It contains a wealth of solutions to problems faced by those who care about the security of their applications. It covers a wide range of topics, including safe initialization, access control, input validation, symmetric and public key cryptography, cryptographic hashes and MACs, authentication and key exchange, PKI, random numbers, and anti-tampering. The rich set of code samples provided in the book's more than 200 recipes will help programmers secure the C and C++ programs they write for both Unix® (including Linux®) and Windows® environments. Readers will learn:

Offering developers an inexpensive way to include testing as part of the development cycle, this cookbook features scores of recipes for testing Web applications, from relatively simple solutions to complex ones that combine several solutions.

????????????????,????????????????,?????????Web????????????,?????Web????????????????????

????????????????????????????????,????C++????????????????????????????????????

These puzzles and mind-benders serve as a way to train logic and help developers, hackers, and system administrators discover unconventional solutions to common IT problems. Users will learn to find bugs in source code, write exploits, and solve nonstandard coding tasks and hacker puzzles. Cryptographic puzzles, puzzles for Linux and Windows hackers, coding puzzles, and puzzles for web designers are included.

A guide to ActionScript covers such topics as runtime, color, drawing, masking, arrays, movie clips, strings, and sound.

This book constitutes the thoroughly refereed proceedings of the Second International Conference on Context-Aware Systems and Applications, ICCASA 2013, held in Phu Quoc Island, Vietnam in November 2013. The 36 revised full papers presented were carefully selected and reviewed from over 100 submissions and cover a wide spectrum of issues in the area of context-aware systems (CAS) and context-based recommendation systems.

?????LINUX????????????????,?????????LINUX?????????????:LINUX?????????????LINUX?????????????????Shell?Shell scripts?????,LINUX?????LINUX???????

???“TM”?????

Based around a theme of the construction of a game engine, this textbook is for final year undergraduate and graduate students, emphasising formal methods in writing robust code quickly.

This book takes an unusual, engineering-inspired approach to illuminate the creation and verification of large software systems . Where other textbooks discuss business practices through generic project management techniques or detailed rigid logic systems, this book examines the interaction between code in a physical machine and the logic applied in creating the software. These elements create an informal and rigorous study of logic, algebra, and geometry through software. Assuming prior experience with C, C++, or Java programming languages, chapters introduce UML, OCL, and Z from scratch. Extensive worked examples motivate readers to learn the languages through the technical side of software science.

A guide to computer software security covers such topics as format string problems, command injection, cross-site scripting, SSL, information leakage, and key exchange.

The only comprehensive set of guidelines for secure Java programming - from the field's leading organizations, CERT and Oracle ••Authoritative, end-to-end code-level requirements for building secure systems with any recent version of Java, including the new Java 7 •Presents techniques that also improve safety, reliability, dependability, robustness, availability, maintainability, and other attributes of quality. •Includes extensive risk assessment guidance, plus references for further information. This is the first authoritative, comprehensive compilation of code-level requirements for building secure systems in Java. Organized by CERT's pioneering software security experts, with support from Oracle's own Java platform developers, it covers every facet of secure software coding with Java 7 SE and Java 6 SE, and offers value even to developers working with other Java versions. The authors itemize the most common coding errors leading to vulnerabilities in Java programs, and provide specific guidelines for avoiding each of them. They show how to produce programs that are not only secure, but also safer, more reliable, more robust, and easier to maintain. After a high-level introduction to Java application security, eighteen consistently-organized chapters detail specific guidelines for each facet of Java development. Each set of guidelines defines conformance, presents both noncompliant examples and corresponding compliant solutions, shows how to assess risk, and offers references for further information. To limit this book's size, the authors focus on 'normative requirements': strict rules for what programmers must do for their work to be secure, as defined by conformance to specific standards that can be tested through automated analysis software. (Note: A follow-up book will present 'non-normative requirements': recommendations for what Java developers typically 'should' do to further strengthen program security beyond testable 'requirements.')

????????????,????????????C++????????,????????????,??,????????????????????,????????????????
?????:?????

[Copyright: f32bcd62b9fe3ac540c80d989c363cb7](https://www.copyright.com/copyright?id=60254080)