

Secure Coding In C And C Sei Series In Software Engineering Paperback

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'.)

Despite their myriad manifestations and different targets, nearly all attacks on computer systems have one fundamental cause: the code used to run far too many systems today is not secure. Flaws in its design, implementation, testing, and operations allow attackers all-too-easy access. "Secure Coding, by Mark G. Graff and Ken vanWyk, looks at the problem of bad code in a new way. Packed with advice based on the authors' decades of experience in the computer security field, this concise and highly readable book explains why so much code today is filled with vulnerabilities, and tells readers what they must do to avoid writing code that can be exploited by attackers. Beyond the technical, "Secure Coding sheds new light on the economic, psychological, and sheer practical reasons why security vulnerabilities are so ubiquitous today. It presents a new way of thinking about these vulnerabilities and ways that developers can compensate for the factors that have produced such unsecured software in the past. It issues a challenge to all those concerned about computer security to finally make a commitment to building code the right way.

Password sniffing, spoofing, buffer overflows, and denial of service: these are only a few of the attacks on today's computer systems and networks. Almost every network security problem actually results from security problems in the underlying software. Writing robust software is difficult -- making that software secure, as well, requires expertise that few developers have. The 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 in such areas as safe initialization, access control, input validation, cryptography, authentication, key exchange, public key infrastructure (PKI), random numbers, and anti-tampering. The rich set of code samples provided in 200-plus recipes will help developers secure the C and C++ programs they write for both Unix (including Linux) and Windows. Book jacket.

Network programming has always been a demanding task. With full-featured and well documented libraries all the way up the stack, Python makes network programming the enjoyable experience it should be. Starting with a walkthrough of today's major networking protocols, with this book you'll learn how to employ Python for network programming, how to request and retrieve web resources, and how to extract data in major formats over the Web. You'll utilize Python for e-mailing using different protocols and you'll interact with remote systems and IP and DNS networking. As the book progresses, socket programming will be covered, followed by how to design servers and the pros and cons of multithreaded and event-driven architectures. You'll develop practical client-side applications, including web API clients, e-mail clients, SSH, and FTP. These applications will also be implemented through existing web application frameworks. A code companion developers will turn to again and again as they seek to protect their systems from attackers.

A detailed introduction to the C programming language for experienced programmers. The world runs on code written in the C programming language, yet most schools begin the curriculum with Python or Java. Effective C bridges this gap and brings C into the modern era--covering the modern C17 Standard as well as potential C2x features. With the aid of this instant classic, you'll soon be writing professional, portable, and secure C programs to power robust systems and solve real-world problems. Robert C. Seacord introduces C and the C Standard Library while addressing best practices, common errors, and open debates in the C community. Developed together with other C Standards committee experts, Effective C will teach you how to debug, test, and analyze C programs. You'll benefit from Seacord's concise explanations of C language constructs and behaviors, and from his 40 years of coding experience. You'll learn: • How to identify and handle undefined behavior in a C program • The range and representations of integers and floating-point values • How dynamic memory allocation works and how to use nonstandard functions • How to use character encodings and types • How to perform I/O with terminals and filesystems using C Standard streams and POSIX file descriptors • How to understand the C compiler's translation phases and the role of the preprocessor • How to test, debug, and analyze C programs Effective C will teach you how to write professional, secure, and portable C code that will stand the test of time and help strengthen the foundation of the computing world.

In a concise and direct question-and-answer format, C++ FAQs, Second Edition brings you the most efficient solutions to more than four hundred of the practical programming challenges you face every day. Moderators of the on-line C++ FAQ at comp.lang.c++, Marshall Cline, Greg Lomow, and Mike Girou are familiar with C++ programmers' most pressing

concerns. In this book, the authors concentrate on those issues most critical to the professional programmer's work, and they present more explanatory material and examples than is possible on-line. This book focuses on the effective use of C++, helping programmers avoid combining seemingly legal C++ constructs in incompatible ways. This second edition is completely up-to-date with the final ANSI/ISO C++ Standard. It covers some of the smaller syntax changes, such as "mutable"; more significant changes, such as RTTI and namespaces; and such major innovations as the C++ Standard Library, including the STL. In addition, this book discusses technologies such as Java, CORBA, COM/COM+, and ActiveX—and the relationship all of these have with C++. These new features and technologies are iconed to help you quickly find what is new and different in this edition. Each question-and-answer section contains an overview of the problem and solution, fuller explanations of concepts, directions for proper use of language features, guidelines for best practices and practices to avoid, and plenty of working, stand-alone examples. This edition is thoroughly cross-referenced and indexed for quick access. Get a value-added service! Try out all the examples from this book at www.codesaw.com. CodeSaw is a free online learning tool that allows you to experiment with live code from your book right in your browser.

“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

Covers topics such as the importance of secure systems, threat modeling, canonical representation issues, solving database input, denial-of-service attacks, and security code reviews and checklists.

With the spread of web-enabled desktop clients and web-server based applications, developers can no longer afford to treat security as an afterthought. It's one topic, in fact, that .NET forces you to address, since Microsoft has placed security-related features at the core of the .NET Framework. Yet, because a developer's carelessness or lack of experience can still allow a program to be used in an unintended way, Programming .NET Security shows you how the various tools will help you write secure applications. The book works as both a comprehensive tutorial and reference to security issues for .NET application development, and contains numerous practical examples in both the C# and VB.NET languages. With Programming .NET Security, you will learn to apply sound security principles to your application designs, and to understand the concepts of identity, authentication and authorization and how they apply to .NET security. This guide also teaches you to: use the .NET run-time security features and .NET security namespaces and types to implement best-practices in your applications, including evidence, permissions, code identity and security policy, and role based and Code Access Security (CAS) use the .NET cryptographic APIs, from hashing and common encryption algorithms to digital signatures and cryptographic keys, to protect your data. use COM+ component services in a secure manner If you program with ASP.NET will also learn how to apply security to your applications. And the book also shows you how to use the Windows Event Log Service to audit Windows security violations that may be a threat to your solution. Authors Adam Freeman and Allen Jones, early .NET adopters and long-time proponents of an "end-to-end" security model, based this book on their years of experience in applying security policies and developing products for NASDAQ, Sun Microsystems, Netscape, Microsoft, and others. With the .NET platform placing security at center stage, the better informed you are, the more secure your project will be.

The First Expert Guide to Static Analysis for Software Security! Creating secure code requires more than just good intentions. Programmers need to know that their code will be safe in an almost infinite number of scenarios and configurations. Static source code analysis gives users the ability to review their work with a fine-toothed comb and uncover the kinds of errors that lead directly to security vulnerabilities. Now, there's a complete guide to static analysis: how it works, how to integrate it into the software development processes, and how to make the most of it during security code review. Static analysis experts Brian Chess and Jacob West look at the most common types of security defects that occur today. They illustrate main points using Java and C code examples taken from real-world security incidents, showing how coding errors are exploited, how they could have been prevented, and how static analysis can rapidly uncover similar mistakes. This book is for everyone concerned with building more secure software: developers, security engineers, analysts, and testers.

Due to the continuously stream of security breaches two security architects in the Netherlands started a project to harvest good practices for better and faster creating architecture and privacy solution designs. This project resulted in a reference architecture that is aimed to help all security architects and designers worldwide. All kinds of topics that help creating a security or privacy solution architecture are outlined, such as: security and privacy principles, common attack vectors, threat models while in-depth guidelines are also given to evaluate the use of Open Source security and privacy application in various use cases.

SCFM: Secure Coding Field Manual is a must for every programmer assigned to write secure code. SCFM is a desk reference to attacks and programming language mitigations for OWASP Top 10 and CWE/SANS Top 25 security vulnerabilities. Languages covered include Java, C/C++, C#/VB.NET/ASP.NET, COBOL, and PL/SQL & DB2.

This book presents findings from the papers accepted at the Cyber Security Education Stream and Cyber Security Technology Stream of The National Cyber Summit's Research Track, reporting on latest advances on topics ranging from software security to cyber-attack detection and modelling to the use of machine learning in cyber security to legislation and policy to surveying of small businesses to cyber competition, and so on. Understanding the latest capabilities in cyber security ensures users and organizations are best prepared for potential negative events.

This book is of interest to cyber security researchers, educators and practitioners, as well as students seeking to learn about cyber security. Describes how to put software security into practice, covering such topics as risk analysis, coding policies, Agile Methods, cryptographic standards, and threat tree patterns.

A fast-paced, thorough introduction to modern C++ written for experienced programmers. After reading C++ Crash Course, you'll be proficient in the core language concepts, the C++ Standard Library, and the Boost Libraries. C++ is one of the most widely used languages for real-world software. In the hands of a knowledgeable programmer, C++ can produce small, efficient, and readable code that any programmer would be proud of. Designed for intermediate to advanced programmers, C++ Crash Course cuts through the weeds to get you straight to the core of C++17, the most modern revision of the ISO standard. Part 1 covers the core of the C++ language, where you'll learn about everything from types and functions, to the object life cycle and expressions. Part 2 introduces you to the C++ Standard Library and Boost Libraries, where you'll learn about all of the high-quality, fully-featured facilities available to you. You'll cover special utility classes, data structures, and algorithms, and learn how to manipulate file systems and build high-performance programs that communicate over networks. You'll learn all the major features of modern C++, including:

- Fundamental types, reference types, and user-defined types
- The object lifecycle including storage duration, memory management, exceptions, call stacks, and the RAII paradigm
- Compile-time polymorphism with templates and run-time polymorphism with virtual classes
- Advanced expressions, statements, and functions
- Smart pointers, data structures, dates and times, numerics, and probability/statistics facilities
- Containers, iterators, strings, and algorithms
- Streams and files, concurrency, networking, and application development

With well over 500 code samples and nearly 100 exercises, C++ Crash Course is sure to help you build a strong C++ foundation.

An essential element of secure coding in the C programming language is well documented and enforceable coding standards. Coding standards encourage programmers to follow a uniform set of rules and guidelines determined by the requirements of the project and organization, rather than by the programmer's familiarity or preference. Once established, these standards can be used as a metric to evaluate source code (using manual or automated processes). The CERT C Secure Coding Standard provides rules and recommendations for secure coding in the C programming language. The goal of these rules and recommendations is to eliminate insecure coding practices and undefined behaviours that can lead to exploitable vulnerabilities. The application of the secure coding standard will lead to higher-quality systems that are robust and more resistant to attack. The book is intended to be used as a reference by both programming teams and individuals. It is based on the web site created for this standard. While the web site will be dynamic, organizations will need a reference that's fixed in time.

Easy to understand and fun to read, this updated edition of Introducing Python is ideal for beginning programmers as well as those new to the language. Author Bill Lubanovic takes you from the basics to more involved and varied topics, mixing tutorials with cookbook-style code recipes to explain concepts in Python 3. End-of-chapter exercises help you practice what you've learned. You'll gain a strong foundation in the language, including best practices for testing, debugging, code reuse, and other development tips. This book also shows you how to use Python for applications in business, science, and the arts, using various Python tools and open source packages.

Software developers need to worry about security as never before. They need clear guidance on safe coding practices, and that's exactly what this book delivers. The book does not delve deep into theory, or rant about the politics of security. Instead, it clearly and simply lays out the most common threats that programmers need to defend against. It then shows programmers how to make their defense. The book takes a broad focus, ranging over SQL injection, worms and buffer overflows, password security, and more. It sets programmers on the path towards successfully defending against the entire gamut of security threats that they might face.

Password sniffing, spoofing, buffer overflows, and denial of service: these are only a few of the attacks on today's computer systems and networks. At the root of this epidemic is poorly written, poorly tested, and insecure code that puts everyone at risk. Clearly, today's developers need help figuring out how to write code that attackers won't be able to exploit. But writing such code is surprisingly difficult. 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:

- How to avoid common programming errors, such as buffer overflows, race conditions, and format string problems
- How to properly SSL-enable applications
- How to create secure channels for client-server communication without SSL
- How to integrate Public Key Infrastructure (PKI) into applications
- Best practices for using cryptography properly
- Techniques and strategies for properly validating input to programs
- How to launch programs securely
- How to use file access mechanisms properly
- Techniques for protecting applications from reverse engineering

The book's web site supplements the book by providing a place to post new recipes, including those written in additional languages like Perl, Java, and Python. Monthly prizes will reward the best recipes submitted by readers. Secure Programming Cookbook for C and C++ is destined to become an essential part of any developer's library, a code companion developers will turn to again and again as they seek to protect their systems from attackers and reduce the risks they face in today's dangerous world.

Despite using them every day, most software engineers know little about how programming languages are designed and implemented. For many, their only experience with that corner of computer science was a terrifying "compilers" class that they suffered through in undergrad and tried to blot from their memory as soon as they had scribbled their last NFA to DFA conversion on the final exam. That fearsome reputation belies a field that is rich with useful techniques and not so difficult as some of its practitioners might have you believe. A better understanding of how programming languages are built will make you a stronger software engineer and teach you concepts and data structures you'll use the rest of your coding days. You might even have fun. This book teaches you everything you need to know to implement a full-featured, efficient scripting language. You'll learn both high-level concepts around parsing and semantics and gritty details like bytecode representation and garbage collection. Your brain will light up with new ideas, and your hands will get dirty and calloused. Starting from main(), you will build a language that features rich syntax, dynamic typing, garbage collection, lexical scope, first-class functions, closures, classes, and inheritance. All packed into a few thousand lines of clean, fast code that you thoroughly understand because you wrote each one yourself.

"Organizations worldwide rely on Java code to perform mission-critical tasks, and therefore that code must be reliable, robust, fast, maintainable, and secure. Java™ Coding Guidelines brings together expert guidelines, recommendations, and code examples to help you meet these demands."--Publisher description.

"I'm an enthusiastic supporter of the CERT Secure Coding Initiative. Programmers have lots of sources of advice on correctness, clarity, maintainability, performance, and even safety. Advice on how specific language features affect security has been missing. The CERT® C Secure Coding Standard fills this need."—Randy Meyers, Chairman of ANSI C "For years we have relied upon the CERT/CC to publish advisories documenting an endless stream of security problems. Now CERT has embodied the advice of leading technical experts to give programmers and managers the practical guidance needed to avoid those problems in new applications and to help secure legacy systems. Well done!"—Dr. Thomas Plum, founder of Plum Hall, Inc. "Connectivity has sharply increased the need for secure, hacker-safe applications. By combining this CERT standard with other safety guidelines, customers gain all-round protection and approach the goal of zero-defect

software.” –Chris Tapp, Field Applications Engineer, LDRA Ltd. “I’ve found this standard to be an indispensable collection of expert information on exactly how modern software systems fail in practice. It is the perfect place to start for establishing internal secure coding guidelines. You won’t find this information elsewhere, and, when it comes to software security, what you don’t know is often exactly what hurts you.” –John McDonald, coauthor of *The Art of Software Security Assessment* Software security has major implications for the operations and assets of organizations, as well as for the welfare of individuals. To create secure software, developers must know where the dangers lie. Secure programming in C can be more difficult than even many experienced programmers believe. This book is an essential desktop reference documenting the first official release of The CERT® C Secure Coding Standard . The standard itemizes those coding errors that are the root causes of software vulnerabilities in C and prioritizes them by severity, likelihood of exploitation, and remediation costs. Each guideline provides examples of insecure code as well as secure, alternative implementations. If uniformly applied, these guidelines will eliminate the critical coding errors that lead to buffer overflows, format string vulnerabilities, integer overflow, and other common software vulnerabilities.

Become a pro at securing your Python apps with this step-by-step guide
About This Book* Get the only book on the market that will help you master Python security* Make your programs more robust, secure, and safe for complex-level applications* This book provides various approaches to securing code that will enable you to implement solutions from the word go
Who This Book Is For This book is aimed at Python developers who want to make their programs secure. Basic knowledge of Python is expected.
What You Will Learn* Simulate various attack scenarios* Perform vulnerability testing using various tools and techniques* Use bruteforce to automate data mining* Identify and mitigate attacks with various OWASP projects* Perform recon and scanning automation to build your own security toolkit* Find about phishing and fuzzing in Python* Conduct network forensic analysis and packet analysis* Work through offensive programming techniques to keep your code clean and precise
In Detail Python is used for a lot of applications, ranging from building web applications and enterprise application to the world of big data. With everyday attacks on applications by hackers, securing applications has become a critical component for Python developers. Starting with the basics to ensure the fundamentals required for security, you will gradually move on to automating various web application attacks, which can then be used by security engineers to perform automated tests. You will mitigate various application security vulnerabilities and explore the defense mechanisms available for developers in Python. You will then learn about the various phases of network security testing that can be automated and how an engineer can simulate various attacks in controlled manner to scan for vulnerabilities. Next, you will learn how to automate password cracking using Python and focus on fuzzing, a key concept of exploit writing and protocol analysis. After reading this book, you will be able to secure your programs and applications and be ready for any kind of spyware and malware.

"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

PRACTICAL, EXAMPLE-RICH COVERAGE OF: Classes, Objects, Encapsulation, Inheritance, Polymorphism Integrated OOP Case Studies: Time, GradeBook, Employee Industrial-Strength, 95-Page OOD/UML® 2 ATM Case Study Standard Template Library (STL): Containers, Iterators and Algorithms I/O, Types, Control Statements, Functions Arrays, Vectors, Pointers, References String Class, C-Style Strings Operator Overloading, Templates Exception Handling, Files Bit and Character Manipulation Boost Libraries and the Future of C++ GNU™ and Visual C++® Debuggers And more... VISIT WWW.DEITEL.COM For information on Deitel® Dive-Into® Series corporate training courses offered at customer sites worldwide (or write to deitel@deitel.com) Download code examples Check out the growing list of programming, Web 2.0 and software-related Resource Centers To receive updates for this book, subscribe to the free DEITEL® BUZZ ONLINE e-mail newsletter at www.deitel.com/newsletter/subscribe.html Read archived issues of the DEITEL® BUZZ ONLINE The professional programmer's DEITEL® guide to C++ and object-oriented application development Written for programmers with a background in high-level language programming, this book applies the Deitel signature live-code approach to teaching programming and explores the C++ language and C++ Standard Libraries in depth. The book presents the concepts in the context of fully tested programs, complete with syntax shading, code highlighting, code walkthroughs and program outputs. The book features 240 C++ applications with over 15,000 lines of proven C++ code, and hundreds of tips that will help you build robust applications. Start with an introduction to C++ using an early classes and objects approach, then rapidly move on to more advanced topics, including templates, exception handling, the Standard Template Library (STL) and selected features from the Boost libraries. You'll enjoy the Deitels' classic treatment of object-oriented programming and the OOD/UML® 2 ATM case study, including a complete C++ implementation. When you're finished, you'll have everything you need to build object-oriented C++ applications. The DEITEL® Developer Series is designed for practicing programmers. The series presents focused treatments of emerging technologies, including C++, .NET, Java™, web services, Internet and web development and more. **PRE-PUBLICATION REVIEWER TESTIMONIALS** "An excellent 'objects first' coverage of C++. The example-driven presentation is enriched by the optional UML case study that contextualizes the material in an ongoing software engineering project." –Gavin Osborne, Saskatchewan Institute of Applied Science and Technology "Introducing the UML early on is a great idea." –Raymond Stephenson, Microsoft "Good use of diagrams, especially of the activation call stack and recursive functions." –Amar Raheja, California State Polytechnic University, Pomona "Terrific discussion of pointers—probably the best I have seen." –Anne B. Horton, Lockheed Martin "Great coverage of polymorphism and how the compiler implements polymorphism 'under the hood.'" –Ed James-Beckham, Borland "The Boost/C++0x chapter will get you up and running quickly with the memory management and regular expression libraries, plus whet your appetite for new C++ features being standardized." –Ed Brey, Kohler Co. "Excellent introduction to the Standard Template Library (STL). The best book

on C++ programming!” –Richard Albright, Goldey-Beacom College “Just when you think you are focused on learning one topic, suddenly you discover you’ve learned more than you expected.” –Chad Willwerth, University of Washington, Tacoma “The most thorough C++ treatment I’ve seen. Replete with real-world case studies covering the full software development lifecycle. Code examples are extraordinary!” –Terrell Hull, Logicalis Integration Solutions/

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.

Learn how to secure your ASP.NET Core web app through robust and secure code Key Features Discover the different types of security weaknesses in ASP.NET Core web applications and learn how to fix them Understand what code makes an ASP.NET Core web app unsafe Build your secure coding knowledge by following straightforward recipes Book Description ASP.NET Core developers are often presented with security test results showing the vulnerabilities found in their web apps. While the report may provide some high-level fix suggestions, it does not specify the exact steps that you need to take to resolve or fix weaknesses discovered by these tests. In *ASP.NET Secure Coding Cookbook*, you'll start by learning the fundamental concepts of secure coding and then gradually progress to identifying common web app vulnerabilities in code. As you progress, you'll cover recipes for fixing security misconfigurations in ASP.NET Core web apps. The book further demonstrates how you can resolve different types of Cross-Site Scripting. A dedicated section also takes you through fixing miscellaneous vulnerabilities that are no longer in the OWASP Top 10 list. This book features a recipe-style format, with each recipe containing sample unsecure code that presents the problem and corresponding solutions to eliminate the security bug. You'll be able to follow along with each step of the exercise and use the accompanying sample ASP.NET Core solution to practice writing secure code. By the end of this book, you'll be able to identify unsecure code causing different security flaws in ASP.NET Core web apps and you'll have gained hands-on experience in removing vulnerabilities and security defects from your code. What you will learn Understand techniques for squashing an ASP.NET Core web app security bug Discover different types of injection attacks and understand how you can prevent this vulnerability from being exploited Fix security issues in code relating to broken authentication and authorization Eliminate the risks of sensitive data exposure by getting up to speed with numerous protection techniques Prevent security misconfiguration by enabling ASP.NET Core web application security features Explore other ASP.NET web application vulnerabilities and secure coding best practices Who this book is for This ASP.NET Core book is for intermediate-level ASP.NET Core web developers and software engineers who use the framework to develop web applications and are looking to focus on their security using coding best practices. The book is also for application security engineers, analysts, and specialists who want to know more about securing ASP.NET Core using code and understand how to resolve issues identified by the security tests they perform daily. The C++11 standard allows programmers to express ideas more clearly, simply, and directly, and to write faster, more efficient code. Bjarne Stroustrup, the designer and original implementer of C++, thoroughly covers the details of this language and its use in his definitive reference, *The C++ Programming Language, Fourth Edition*. In *A Tour of C++*, Stroustrup excerpts the overview chapters from that complete reference, expanding and enhancing them to give an experienced programmer—in just a few hours—a clear idea of what constitutes modern C++. In this concise, self-contained guide, Stroustrup covers most major language features and the major standard-library components—not, of course, in great depth, but to a level that gives programmers a meaningful overview of the language, some key examples, and practical help in getting started. Stroustrup presents the C++ features in the context of the programming styles they support, such as object-oriented and generic programming. His tour is remarkably comprehensive. Coverage begins with the basics, then ranges widely through more advanced topics, including many that are new in C++11, such as move semantics, uniform initialization, lambda expressions, improved containers, random numbers, and concurrency. The tour ends with a discussion of the design and evolution of C++ and the extensions added for C++11. This guide does not aim to teach you how to program (see Stroustrup's *Programming: Principles and Practice Using C++* for that); nor will it be the only resource you'll need for C++ mastery (see Stroustrup's *The C++ Programming Language, Fourth Edition*, for that). If, however, you are a C or C++ programmer wanting greater familiarity with the current C++ language, or a programmer versed in another language wishing to gain an accurate picture of the nature and benefits of modern C++, you can't find a shorter or simpler introduction than this tour provides.

Stop manually analyzing binary! *Practical Binary Analysis* is the first book of its kind to present advanced binary analysis topics, such as binary instrumentation, dynamic taint analysis, and symbolic execution, in an accessible way. As malware increasingly obfuscates itself and applies anti-analysis techniques to thwart our analysis, we need more sophisticated methods that allow us to raise that dark curtain designed to keep us out--binary analysis can help. The goal of all binary analysis is to determine (and possibly modify) the true properties of binary programs to understand what they really do, rather than what we think they should do. While reverse engineering and disassembly are critical first steps in many forms of binary analysis, there is much more to be learned. This hands-on guide teaches you how to tackle the fascinating but challenging topics of binary analysis and instrumentation and helps you become proficient in an area typically only mastered by a small group of expert hackers. It will take

you from basic concepts to state-of-the-art methods as you dig into topics like code injection, disassembly, dynamic taint analysis, and binary instrumentation. Written for security engineers, hackers, and those with a basic working knowledge of C/C++ and x86-64, Practical Binary Analysis will teach you in-depth how binary programs work and help you acquire the tools and techniques needed to gain more control and insight into binary programs. Once you've completed an introduction to basic binary formats, you'll learn how to analyze binaries using techniques like the GNU/Linux binary analysis toolchain, disassembly, and code injection. You'll then go on to implement profiling tools with Pin and learn how to build your own dynamic taint analysis tools with libdft and symbolic execution tools using Triton. You'll learn how to:

- Parse ELF and PE binaries and build a binary loader with libbfd
- Use data-flow analysis techniques like program tracing, slicing, and reaching definitions analysis to reason about runtime flow of your programs
- Modify ELF binaries with techniques like parasitic code injection and hex editing
- Build custom disassembly tools with Capstone
- Use binary instrumentation to circumvent anti-analysis tricks commonly used by malware
- Apply taint analysis to detect control hijacking and data leak attacks
- Use symbolic execution to build automatic exploitation tools

With exercises at the end of each chapter to help solidify your skills, you'll go from understanding basic assembly to performing some of the most sophisticated binary analysis and instrumentation. Practical Binary Analysis gives you what you need to work effectively with binary programs and transform your knowledge from basic understanding to expert-level proficiency.

The CERT C Coding Standard, Second Edition enumerates the coding errors that are the root causes of current software vulnerabilities in C, prioritizing them by severity, likelihood of exploitation, and remediation costs. "Secure programming in C can be more difficult than even many experienced programmers realize," said Robert C. Seacord, technical manager of the CERT Secure Coding Initiative and author of the CERT C Coding Standard. "Software systems are becoming increasingly complex as our dependency on these systems increases. In our new CERT standard, as with all of our standards, we identify insecure coding practices and present secure alternatives that software developers can implement to reduce or eliminate vulnerabilities before deployment."

Learn how to identify and code around weaknesses in the C programming language to write more secure programs.

Describes how to put software security into practice, covering such topics as risk management frameworks, architectural risk analysis, security testing, and penetration testing.

The official book on the Rust programming language, written by the Rust development team at the Mozilla Foundation, fully updated for Rust 2018. The Rust Programming Language is the official book on Rust: an open source systems programming language that helps you write faster, more reliable software. Rust offers control over low-level details (such as memory usage) in combination with high-level ergonomics, eliminating the hassle traditionally associated with low-level languages. The authors of The Rust Programming Language, members of the Rust Core Team, share their knowledge and experience to show you how to take full advantage of Rust's features--from installation to creating robust and scalable programs. You'll begin with basics like creating functions, choosing data types, and binding variables and then move on to more advanced concepts, such as:

- Ownership and borrowing, lifetimes, and traits
- Using Rust's memory safety guarantees to build fast, safe programs
- Testing, error handling, and effective refactoring
- Generics, smart pointers, multithreading, trait objects, and advanced pattern matching
- Using Cargo, Rust's built-in package manager, to build, test, and document your code and manage dependencies
- How best to use Rust's advanced compiler with compiler-led programming techniques

You'll find plenty of code examples throughout the book, as well as three chapters dedicated to building complete projects to test your learning: a number guessing game, a Rust implementation of a command line tool, and a multithreaded server. New to this edition: An extended section on Rust macros, an expanded chapter on modules, and appendixes on Rust development tools and editions.

What every software professional should know about security. Designing Secure Software consolidates Loren Kohnfelder's more than twenty years of experience into a concise, elegant guide to improving the security of technology products. Written for a wide range of software professionals, it emphasizes building security into software design early and involving the entire team in the process. The book begins with a discussion of core concepts like trust, threats, mitigation, secure design patterns, and cryptography. The second part, perhaps this book's most unique and important contribution to the field, covers the process of designing and reviewing a software design with security considerations in mind. The final section details the most common coding flaws that create vulnerabilities, making copious use of code snippets written in C and Python to illustrate implementation vulnerabilities. You'll learn how to:

- Identify important assets, the attack surface, and the trust boundaries in a system
- Evaluate the effectiveness of various threat mitigation candidates
- Work with well-known secure coding patterns and libraries
- Understand and prevent vulnerabilities like XSS and CSRF, memory flaws, and more
- Use security testing to proactively identify vulnerabilities introduced into code
- Review a software design for security flaws effectively and without judgment

Kohnfelder's career, spanning decades at Microsoft and Google, introduced numerous software security initiatives, including the co-creation of the STRIDE threat modeling framework used widely today. This book is a modern, pragmatic consolidation of his best practices, insights, and ideas about the future of software.

"The security of information systems has not improved at a rate consistent with the growth and sophistication of the attacks being made against them. To address this problem, we must improve the underlying strategies and techniques used to create our systems. Specifically, we must build security in from the start, rather than append it as an afterthought. That's the point of Secure Coding in C and C++. In careful detail, this book shows software developers how to build high-quality systems that are less vulnerable to costly and even catastrophic attack. It's a book that every developer should read before the start of any serious project." --Frank Abagnale, author, lecturer, and leading consultant on fraud prevention and secure documents

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 nearly 18,000 vulnerability reports over the past ten years, the CERT/Coordination Center (CERT/CC) has determined that a relatively small number of root causes account for most of them. This book identifies and explains these causes and shows the steps that can be taken to prevent exploitation. Moreover, this book encourages programmers to adopt security best practices and develop a security mindset that can help protect software from tomorrow's attacks, not just today's. Drawing on the CERT/CC's reports and conclusions, Robert 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/C++ application
- Thwart buffer overflows and stack-smashing 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: integer overflows, sign errors, and truncation errors
- Correctly use formatted output functions without introducing format-string vulnerabilities
- Avoid I/O vulnerabilities, including race conditions

Secure Coding in C and C++ 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.

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.

The book is logically divided into 5 main categories with each category representing a major skill set required by most security professionals:

1. Coding – The ability to program and script is quickly becoming a mainstream requirement for just about everyone in the security industry. This section covers the basics in coding complemented with a slue of programming tips and tricks in C/C++, Java, Perl and NASL.
2. Sockets – The technology that allows programs and scripts to communicate over a network is sockets. Even though the theory remains the same – communication over TCP and UDP, sockets are implemented differently in nearly ever language.
3. Shellcode – Shellcode, commonly defined as bytecode converted from Assembly, is utilized to execute commands on remote systems via direct memory access.
4. Porting – Due to the differences between operating platforms and language implementations on those platforms, it is a common practice to modify an original body of code to work on a different platforms. This technique is known as porting and is incredible useful in the real world environments since it allows you to not “recreate the wheel.
5. Coding Tools – The culmination of the previous four sections, coding tools brings all of the techniques that you have learned to the forefront. With the background technologies and techniques you will now be able to code quick utilities that will not only make you more productive, they will arm you with an extremely valuable skill that will remain with you as long as you make the proper time and effort dedications. *Contains never before seen chapters on writing and automating exploits on windows systems with all-new exploits. *Perform zero-day exploit forensics by reverse engineering malicious code. *Provides working code and scripts in all of the most common programming languages for readers to use TODAY to defend their networks.

[Copyright: 81f232ebc06e2f228ce22a6b911dccec](#)