

## Security With Go Explore The Power Of Golang To Secure Host Web And Cloud Services

Summary Securing DevOps explores how the techniques of DevOps and security should be applied together to make cloud services safer. This introductory book reviews the latest practices used in securing web applications and their infrastructure and teaches you techniques to integrate security directly into your product. You'll also learn the core concepts of DevOps, such as continuous integration, continuous delivery, and infrastructure as a service. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications.

About the Technology An application running in the cloud can benefit from incredible efficiencies, but they come with unique security threats too. A DevOps team's highest priority is understanding those risks and hardening the system against them. About the Book Securing DevOps teaches you the essential techniques to secure your cloud services. Using compelling case studies, it shows you how to build security into automated testing, continuous delivery, and other core DevOps processes. This experience-rich book is filled with mission-critical strategies to protect web applications against attacks, deter fraud attempts, and make your services safer when operating at scale. You'll also learn to identify, assess, and secure the unique vulnerabilities posed by cloud deployments and automation tools commonly used in modern infrastructures. What's inside An approach to continuous security Implementing test-driven security in DevOps Security techniques for cloud services Watching for fraud and responding to incidents Security testing and risk assessment About the Reader Readers should be comfortable with Linux and standard DevOps practices like CI, CD, and unit testing. About the Author Julien Vehent is a security architect and DevOps advocate. He leads the Firefox Operations Security team at Mozilla, and is responsible for the security of Firefox's high-traffic cloud services and public websites. Table of Contents Securing DevOps PART 1 - Case study: applying layers of security to a simple DevOps pipeline Building a barebones DevOps pipeline Security layer 1: protecting web applications Security layer 2: protecting cloud infrastructures Security layer 3: securing communications Security layer 4: securing the delivery pipeline PART 2 - Watching for anomalies and protecting services against attacks Collecting and storing logs Analyzing logs for fraud and attacks Detecting intrusions The Caribbean breach: a case study in incident response PART 3 - Maturing DevOps security Assessing risks Testing security Continuous security A tutorial leading the aspiring Go developer to full mastery of Golang's distributed features. Key Features This book provides enough concurrency theory to give you a contextual understanding of Go concurrency It gives weight to synchronous and asynchronous data streams in Golang web applications It makes Goroutines and Channels completely familiar and natural to Go developers Book Description Distributed Computing with Go gives developers with a good idea how basic Go development works the tools to fulfill the true potential of Golang development in a world of concurrent web and cloud applications. Nikhil starts out by setting up a professional Go development environment. Then you'll learn the basic concepts and practices of Golang concurrent and parallel development. You'll find out in the new few chapters how to balance resources and data with REST and standard web approaches while keeping concurrency in mind. Most Go applications these days will run in a data center or on the cloud, which is a condition upon which the next chapter depends. There, you'll expand your skills considerably by writing a distributed document indexing system during the next two chapters. This system has to balance a large corpus of documents with considerable analytical demands. Another use case is the way in which a web application written in Go can be consciously redesigned to take distributed features into account. The chapter is rather interesting for Go developers who have to migrate existing Go applications to computationally and memory-intensive environments. The final chapter relates to the rather onerous task of testing parallel and distributed applications, something that is not usually taught in standard computer science curricula. What you will learn Gain proficiency with concurrency and parallelism in Go Learn how to test your application using Go's standard library Learn industry best practices with technologies such as REST, OpenAPI, Docker, and so on Design and build a distributed search engine Learn strategies on how to design a system for web scale Who this book is for This book is for developers who are familiar with the Golang syntax and have a good idea of how basic Go development works. It would be advantageous if you have been through a web application product cycle, although it's not necessary.

Summary Get Programming with Go introduces you to the powerful Go language without confusing jargon or high-level theory. By working through 32 quick-fire lessons, you'll quickly pick up the basics of the innovative Go programming language! Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the Technology Go is a small programming language designed by Google to tackle big problems. Large projects mean large teams with people of varying levels of experience. Go offers a small, yet capable, language that can be understood and used by anyone, no matter their experience. About the Book Hobbyists, newcomers, and professionals alike can benefit from a fast, modern language; all you need is the right resource! Get Programming with Go provides a hands-on introduction to Go language fundamentals, serving as a solid foundation for your future programming projects. You'll master Go syntax, work with types and functions, and explore bigger ideas like state and concurrency, with plenty of exercises to lock in what you learn. What's inside Language concepts like slices, interfaces, pointers, and concurrency Seven capstone projects featuring spacefaring gophers, Mars rovers, ciphers, and simulations All examples run in the Go Playground - no installation required! About the Reader This book is for anyone familiar with computer programming, as well as anyone with the desire to learn. About the Author Nathan Youngman organizes the Edmonton Go meetup and is a mentor with Canada Learning Code. Roger Peppé contributes to Go and runs the Newcastle upon Tyne Go meetup. Table of Contents Unit 0 - GETTING STARTED Get ready, get set, Go Unit 1 - IMPERATIVE PROGRAMMING A glorified calculator Loops and branches Variable scope Capstone: Ticket to Mars Unit 2 - TYPES Real numbers Whole numbers Big numbers Multilingual text Converting between types Capstone: The Vigenère cipher Unit 3 - BUILDING BLOCKS Functions Methods First-class functions Capstone: Temperature tables Unit 4 - COLLECTIONS Arrayed in splendor Slices: Windows into arrays A bigger slice The ever-versatile map Capstone: A slice of life Unit 5 - STATE AND BEHAVIOR A little structure Go's got no class Composition and forwarding Interfaces Capstone: Martian animal sanctuary Unit 6 - DOWN THE GOPHER HOLE A few pointers Much ado about nil To err is human Capstone: Sudoku rules Unit 7 - CONCURRENT PROGRAMMING Goroutines and concurrency Concurrent state Capstone: Life on Mars

"A 22-volume, highly illustrated, A-Z general encyclopedia for all ages, featuring sections on how to use World Book, other research aids, pronunciation key, a student guide to better writing, speaking, and research skills, and comprehensive index"--

Today's parents are constantly pressured to be perfect. But in striving to do everything right, we risk missing what children really need for lifelong emotional security. Now the simple, powerful

"Circle of Security" parenting strategies that Kent Hoffman, Glen Cooper, and Bert Powell have taught thousands of families are available in self-help form for the first time. You will learn: How to balance nurturing and protectiveness with promoting your child's independence. What emotional needs a toddler or older child may be expressing through difficult behavior. How your own upbringing affects your parenting style--and what you can do about it. Filled with vivid stories and unique practical tools, this book puts the keys to healthy attachment within everyone's reach--self-understanding, flexibility, and the willingness to make and learn from mistakes. Self-assessment checklists can be downloaded and printed for ease of use.

Dive into key topics in network architecture and Go, such as data serialization, application level protocols, character sets and encodings. This book covers network architecture and gives an overview of the Go language as a primer, covering the latest Go release. Beyond the fundamentals, Network Programming with Go covers key networking and security issues such as HTTP and HTTPS, templates, remote procedure call (RPC), web sockets including HTML5 web sockets, and more. Additionally, author Jan Newmarch guides you in building and connecting to a complete web server based on Go. This book can serve as both as an essential learning guide and reference on Go networking. What You Will Learn Master network programming with Go Carry out data serialization Use application-level protocols Manage character sets and encodings Deal with HTTP(S) Build a complete Go-based web server Work with RPC, web sockets, and more Who This Book Is For Experienced Go programmers and other programmers with some experience with the Go language.

Increase profitability, elevate work culture, and exceed productivity goals through DevOps practices. More than ever, the effective management of technology is critical for business competitiveness. For decades, technology leaders have struggled to balance agility, reliability, and security. The consequences of failure have never been greater--whether it's the healthcare.gov debacle, cardholder data breaches, or missing the boat with Big Data in the cloud. And yet, high performers using DevOps principles, such as Google, Amazon, Facebook, Etsy, and Netflix, are routinely and reliably deploying code into production hundreds, or even thousands, of times per day. Following in the footsteps of The Phoenix Project, The DevOps Handbook shows leaders how to replicate these incredible outcomes, by showing how to integrate Product Management, Development, QA, IT Operations, and Information Security to elevate your company and win in the marketplace.

The first stop for your security needs when using Go, covering host, network, and cloud security for ethical hackers and defense against intrusion Key Features First introduction to Security with Golang Adopting a Blue Team/Red Team approach Take advantage of speed and inherent safety of Golang Works as an introduction to security for Golang developers Works as a guide to Golang security packages for recent Golang beginners Book Description Go is becoming more and more popular as a language for security experts. Its wide use in server and cloud environments, its speed and ease of use, and its evident capabilities for data analysis, have made it a prime choice for developers who need to think about security. Security with Go is the first Golang security book, and it is useful for both blue team and red team applications. With this book, you will learn how to write secure software, monitor your systems, secure your data, attack systems, and extract information. Defensive topics include cryptography, forensics, packet capturing, and building secure web applications. Offensive topics include brute force, port scanning, packet injection, web scraping, social engineering, and post exploitation techniques. What you will learn Learn the basic concepts and principles of secure programming Write secure Golang programs and applications Understand classic patterns of attack Write Golang scripts to defend against network-level attacks Learn how to use Golang security packages Apply and explore cryptographic methods and packages Learn the art of defending against brute force attacks Secure web and cloud applications Who this book is for Security with Go is aimed at developers with basics in Go to the level that they can write their own scripts and small programs without difficulty. Readers should be familiar with security concepts, and familiarity with Python security applications and libraries is an advantage, but not a necessity.

This highly illustrated, step-by-step guide gives detailed instructions for dozens of different manipulation techniques, covering all levels of the spine, thorax, and pelvis. It also includes a helpful overview of the principles and theory of spinal manipulation and its use in clinical practice. The accompanying DVD contains video clips demonstrating the techniques described in the book. The new edition is a highly illustrated, step-by-step guide to 41 manipulation techniques commonly used in clinical practice. The book also provides the related theory essential for safe and effective use of manipulation techniques.

Whether you're searching for new or additional opportunities, information security can be vast and overwhelming. In this practical guide, author Christina Morillo introduces technical knowledge from a diverse range of experts in the infosec field. Through 97 concise and useful tips, you'll learn how to expand your skills and solve common issues by working through everyday security problems. You'll also receive valuable guidance from professionals on how to navigate your career within this industry. How do you get buy-in from the C-suite for your security program? How do you establish an incident and disaster response plan? This practical book takes you through actionable advice on a wide variety of infosec topics, including thought-provoking questions that drive the direction of the field. Continuously Learn to Protect Tomorrow's Technology--Alyssa Columbus Fight in Cyber Like the Military Fights in the Physical--Andrew Harris Keep People at the Center of Your Work--Camille Stewart Infosec Professionals Need to Know Operational Resilience--Ann Johnson Taking Control of Your Own Journey--Antoine Middleton Security, Privacy, and Messy Data Webs: Taking Back Control in Third-Party Environments--Ben Brook Every Information Security Problem Boils Down to One Thing--Ben Smith Focus on the WHAT and the Why First, Not the Tool--Christina Morillo Deliberately challenging the traditional, state-centric analysis of security, this book focuses on subnational and transnational forces—religious and ethnic conflict, climate change, pandemic diseases, poverty, terrorism, criminal networks, and cyber attacks—that threaten human beings and their communities across state borders. Examining threats related to human security in the modern era of globalization, Reveron and Mahoney-Norris argue that human security is national security today, even for great powers. This fully updated second edition of Human and National Security: Understanding Transnational Challenges builds on the foundation of the first (published as Human Security in a Borderless World) while also incorporating new discussions of the rise of identity politics in an increasingly connected world, an expanded account of the actors, institutions, and approaches to security today, and the ways diverse global actors protect and promote human security. An essential text for security studies and international relations students, Human and

National Security not only presents human security challenges and their policy implications, it also highlights how governments, societies, and international forces can, and do, take advantage of possibilities in the contemporary era to develop a more stable and secure world for all.

API Security in Action teaches you how to create secure APIs for any situation. By following this hands-on guide you'll build a social network API while mastering techniques for flexible multi-user security, cloud key management, and lightweight cryptography. Summary A web API is an efficient way to communicate with an application or service. However, this convenience opens your systems to new security risks. API Security in Action gives you the skills to build strong, safe APIs you can confidently expose to the world. Inside, you'll learn to construct secure and scalable REST APIs, deliver machine-to-machine interaction in a microservices architecture, and provide protection in resource-constrained IoT (Internet of Things) environments. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the technology APIs control data sharing in every service, server, data store, and web client. Modern data-centric designs—including microservices and cloud-native applications—demand a comprehensive, multi-layered approach to security for both private and public-facing APIs. About the book API Security in Action teaches you how to create secure APIs for any situation. By following this hands-on guide you'll build a social network API while mastering techniques for flexible multi-user security, cloud key management, and lightweight cryptography. When you're done, you'll be able to create APIs that stand up to complex threat models and hostile environments. What's inside Authentication Authorization Audit logging Rate limiting Encryption About the reader For developers with experience building RESTful APIs. Examples are in Java. About the author Neil Madden has in-depth knowledge of applied cryptography, application security, and current API security technologies. He holds a Ph.D. in Computer Science. Table of Contents PART 1 - FOUNDATIONS 1 What is API security? 2 Secure API development 3 Securing the Natter API PART 2 - TOKEN-BASED AUTHENTICATION 4 Session cookie authentication 5 Modern token-based authentication 6 Self-contained tokens and JWTs PART 3 - AUTHORIZATION 7 OAuth2 and OpenID Connect 8 Identity-based access control 9 Capability-based security and macaroons PART 4 - MICROSERVICE APIS IN KUBERNETES 10 Microservice APIs in Kubernetes 11 Securing service-to-service APIs PART 5 - APIS FOR THE INTERNET OF THINGS 12 Securing IoT communications 13 Securing IoT APIs

Can a system be considered truly reliable if it isn't fundamentally secure? Or can it be considered secure if it's unreliable? Security is crucial to the design and operation of scalable systems in production, as it plays an important part in product quality, performance, and availability. In this book, experts from Google share best practices to help your organization design scalable and reliable systems that are fundamentally secure. Two previous O'Reilly books from Google—Site Reliability Engineering and The Site Reliability Workbook—demonstrated how and why a commitment to the entire service lifecycle enables organizations to successfully build, deploy, monitor, and maintain software systems. In this latest guide, the authors offer insights into system design, implementation, and maintenance from practitioners who specialize in security and reliability. They also discuss how building and adopting their recommended best practices requires a culture that's supportive of such change. You'll learn about secure and reliable systems through: Design strategies Recommendations for coding, testing, and debugging practices Strategies to prepare for, respond to, and recover from incidents Cultural best practices that help teams across your organization collaborate effectively

The only security book to be chosen as a Dr. Dobbs Jolt Award Finalist since Bruce Schneier's Secrets and Lies and Applied Cryptography! Adam Shostack is responsible for security development lifecycle threat modeling at Microsoft and is one of a handful of threat modeling experts in the world. Now, he is sharing his considerable expertise into this unique book. With pages of specific actionable advice, he details how to build better security into the design of systems, software, or services from the outset. You'll explore various threat modeling approaches, find out how to test your designs against threats, and learn effective ways to address threats that have been validated at Microsoft and other top companies. Systems security managers, you'll find tools and a framework for structured thinking about what can go wrong. Software developers, you'll appreciate the jargon-free and accessible introduction to this essential skill. Security professionals, you'll learn to discern changing threats and discover the easiest ways to adopt a structured approach to threat modeling. Provides a unique how-to for security and software developers who need to design secure products and systems and test their designs Explains how to threat model and explores various threat modeling approaches, such as asset-centric, attacker-centric and software-centric Provides effective approaches and techniques that have been proven at Microsoft and elsewhere Offers actionable how-to advice not tied to any specific software, operating system, or programming language Authored by a Microsoft professional who is one of the most prominent threat modeling experts in the world As more software is delivered on the Internet or operates on Internet-connected devices, the design of secure software is absolutely critical. Make sure you're ready with Threat Modeling: Designing for Security.

This book on computer security threats explores the computer security threats and includes a broad set of solutions to defend the computer systems from these threats. The book is triggered by the understanding that digitalization and growing dependence on the Internet poses an increased risk of computer security threats in the modern world. The chapters discuss different research frontiers in computer security with algorithms and implementation details for use in the real world. Researchers and practitioners in areas such as statistics, pattern recognition, machine learning, artificial intelligence, deep learning, data mining, data analytics and visualization are contributing to the field of computer security. The intended audience of this book will mainly consist of researchers, research students, practitioners, data analysts, and business professionals who seek information on computer security threats and its defensive measures.

Building a Practical Information Security Program provides users with a strategic view on how to build an information security program that aligns with business objectives. The

information provided enables both executive management and IT managers not only to validate existing security programs, but also to build new business-driven security programs. In addition, the subject matter supports aspiring security engineers to forge a career path to successfully manage a security program, thereby adding value and reducing risk to the business. Readers learn how to translate technical challenges into business requirements, understand when to "go big or go home," explore in-depth defense strategies, and review tactics on when to absorb risks. This book explains how to properly plan and implement an infosec program based on business strategy and results. Provides a roadmap on how to build a security program that will protect companies from intrusion Shows how to focus the security program on its essential mission and move past FUD (fear, uncertainty, and doubt) to provide business value Teaches how to build consensus with an effective business-focused program

Defending Assessment Security in a Digital World explores the phenomenon of e-cheating and identifies ways to bolster assessment to ensure that it is secured against threats posed by technology. Taking a multi-disciplinary approach, the book develops the concept of assessment security through research from cybersecurity, game studies, artificial intelligence and surveillance studies. Throughout, there is a rigorous examination of the ways people cheat in different contexts, and the effectiveness of different approaches at stopping cheating. This evidence informs the development of standards and metrics for assessment security, and ways that assessment design can help address e-cheating. Its new concept of assessment security both complements and challenges traditional notions of academic integrity. By focusing on proactive, principles-based approaches, the book equips educators, technologists and policymakers to address both current e-cheating as well as future threats.

AWS Security covers best practices for access policies, data protection, auditing, continuous monitoring, and incident response. To create secure applications and infrastructure on AWS, you need to understand the tools and features the platform provides and learn new approaches to configuring and managing them. AWS Security provides comprehensive coverage of the key tools and concepts you can use to defend AWS-based systems. AWS Security covers best practices for access policies, data protection, auditing, continuous monitoring, and incident response. Through well-documented examples and procedures, you'll explore several deliberately insecure applications, learning the exploits and vulnerabilities commonly used to attack them and the security practices to counter those attacks. With this practical primer, you'll be well prepared to evaluate your system's security, detect threats, and respond with confidence. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications.

Proven methodologies and concurrency techniques that will help you write faster and better code with Go programming Key Features Explore Go's profiling tools to write faster programs by identifying and fixing bottlenecks Address Go-specific performance issues such as memory allocation and garbage collection Delve into the subtleties of concurrency and discover how to successfully implement it in everyday applications Book Description Go is an easy-to-write language that is popular among developers thanks to its features such as concurrency, portability, and ability to reduce complexity. This Golang book will teach you how to construct idiomatic Go code that is reusable and highly performant. Starting with an introduction to performance concepts, you'll understand the ideology behind Go's performance. You'll then learn how to effectively implement Go data structures and algorithms along with exploring data manipulation and organization to write programs for scalable software. This book covers channels and goroutines for parallelism and concurrency to write high-performance code for distributed systems. As you advance, you'll learn how to manage memory effectively. You'll explore the compute unified device architecture (CUDA) application programming interface (API), use containers to build Go code, and work with the Go build cache for quicker compilation. You'll also get to grips with profiling and tracing Go code for detecting bottlenecks in your system. Finally, you'll evaluate clusters and job queues for performance optimization and monitor the application for performance regression. By the end of this Go programming book, you'll be able to improve existing code and fulfill customer requirements by writing efficient programs. What you will learn Organize and manipulate data effectively with clusters and job queues Explore commonly applied Go data structures and algorithms Write anonymous functions in Go to build reusable apps Profile and trace Go apps to reduce bottlenecks and improve efficiency Deploy, monitor, and iterate Go programs with a focus on performance Dive into memory management and CPU and GPU parallelism in Go Who this book is for This Golang book is a must for developers and professionals who have an intermediate-to-advanced understanding of Go programming, and are interested in improving their speed of code execution.

Political Ideologies provides a broad-ranging introduction to both the classical and contemporary political ideologies. Adopting a global outlook, it introduces readers to ideologies' increasingly global reach and the different national versions of these ideologies. Importantly, ideologies are presented as frameworks of interpretation and political commitment, encouraging readers to evaluate how ideologies work in practice, the problematic links between ideas and political action, and the impact of ideologies. Regular learning features encourage readers to think critically about ideologies, and view them as competing and contestable ways of interpreting the world. A unique "stop and think" feature calls for readers to reflect on their own ideological beliefs. Online Resources: Political Ideologies is accompanied by comprehensive online resources, to support political ideology courses. For students: \* Further reading and resources for each chapter to help students to undertake further research and deepen their understanding and critical thinking;\* Regular updates help students to keep up to date with ideologies as frameworks of understanding and political action in the real world. For lecturers: \* Indicative answers to questions in the book provide a framework for approaching these;\* Powerpoint slides to support each chapter, providing an overview and key points to help with planning;\* Further discussion and debate ideas, for use in seminars, encourage big picture thinking about the relationships between ideologies.

To facilitate scalability and resilience, many organizations now run applications in cloud native environments using containers and orchestration. But how do you know if the

deployment is secure? This practical book examines key underlying technologies to help developers, operators, and security professionals assess security risks and determine appropriate solutions. Author Liz Rice, Chief Open Source Officer at Isovalent, looks at how the building blocks commonly used in container-based systems are constructed in Linux. You'll understand what's happening when you deploy containers and learn how to assess potential security risks that could affect your deployments. If you run container applications with kubectl or docker and use Linux command-line tools such as ps and grep, you're ready to get started. Explore attack vectors that affect container deployments Dive into the Linux constructs that underpin containers Examine measures for hardening containers Understand how misconfigurations can compromise container isolation Learn best practices for building container images Identify container images that have known software vulnerabilities Leverage secure connections between containers Use security tooling to prevent attacks on your deployment

This book is for cybersecurity leaders across all industries and organizations. It is intended to bridge the gap between the data center and the board room. This book examines the multitude of communication challenges that CISOs are faced with every day and provides practical tools to identify your audience, tailor your message and master the art of communicating. Poor communication is one of the top reasons that CISOs fail in their roles. By taking the step to work on your communication and soft skills (the two go hand-in-hand), you will hopefully never join their ranks. This is not a “communication theory” book. It provides just enough practical skills and techniques for security leaders to get the job done. Learn fundamental communication skills and how to apply them to day-to-day challenges like communicating with your peers, your team, business leaders and the board of directors. Learn how to produce meaningful metrics and communicate before, during and after an incident. Regardless of your role in Tech, you will find something of value somewhere along the way in this book.

An all-practical guide to the cryptography behind common tools and protocols that will help you make excellent security choices for your systems and applications. In Real-World Cryptography, you will find: Best practices for using cryptography Diagrams and explanations of cryptographic algorithms Implementing digital signatures and zero-knowledge proofs Specialized hardware for attacks and highly adversarial environments Identifying and fixing bad practices Choosing the right cryptographic tool for any problem Real-World Cryptography reveals the cryptographic techniques that drive the security of web APIs, registering and logging in users, and even the blockchain. You'll learn how these techniques power modern security, and how to apply them to your own projects. Alongside modern methods, the book also anticipates the future of cryptography, diving into emerging and cutting-edge advances such as cryptocurrencies, and post-quantum cryptography. All techniques are fully illustrated with diagrams and examples so you can easily see how to put them into practice. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the technology Cryptography is the essential foundation of IT security. To stay ahead of the bad actors attacking your systems, you need to understand the tools, frameworks, and protocols that protect your networks and applications. This book introduces authentication, encryption, signatures, secret-keeping, and other cryptography concepts in plain language and beautiful illustrations. About the book Real-World Cryptography teaches practical techniques for day-to-day work as a developer, sysadmin, or security practitioner. There's no complex math or jargon: Modern cryptography methods are explored through clever graphics and real-world use cases. You'll learn building blocks like hash functions and signatures; cryptographic protocols like HTTPS and secure messaging; and cutting-edge advances like post-quantum cryptography and cryptocurrencies. This book is a joy to read—and it might just save your bacon the next time you're targeted by an adversary after your data. What's inside Implementing digital signatures and zero-knowledge proofs Specialized hardware for attacks and highly adversarial environments Identifying and fixing bad practices Choosing the right cryptographic tool for any problem About the reader For cryptography beginners with no previous experience in the field. About the author David Wong is a cryptography engineer. He is an active contributor to internet standards including Transport Layer Security. Table of Contents PART 1 PRIMITIVES: THE INGREDIENTS OF CRYPTOGRAPHY 1 Introduction 2 Hash functions 3 Message authentication codes 4 Authenticated encryption 5 Key exchanges 6 Asymmetric encryption and hybrid encryption 7 Signatures and zero-knowledge proofs 8 Randomness and secrets PART 2 PROTOCOLS: THE RECIPES OF CRYPTOGRAPHY 9 Secure transport 10 End-to-end encryption 11 User authentication 12 Crypto as in cryptocurrency? 13 Hardware cryptography 14 Post-quantum cryptography 15 Is this it? Next-generation cryptography 16 When and where cryptography fails

Network Programming with Go teaches you how to write clean, secure network software with the programming language designed to make it seem easy. Go combines the best parts of many other programming languages. It's fast, scalable, and designed for high-performance networking and multiprocessing—in other words, it's perfect for network programming. Network Programming with Go is for developers ready to start leveraging Go's ease of use for writing secure, readable, production-ready network code. Early chapters establish a foundation of networking and traffic-routing know-how upon which the rest of the book builds. You'll put that knowledge to use as author Adam Woodbeck guides you through writing programs that communicate using TCP, UDP, Unix sockets, and other features that ensure reliable data transmission. As you progress, you'll explore higher-level network protocols like HTTP and HTTP/2, then build applications that securely interact with servers, clients, and APIs over a network using TLS. In addition, Woodbeck shows you how to create a simple messaging protocol, develop tools for monitoring network traffic, craft a custom web server, and implement best practices for interacting with cloud providers using their SDKs. Along the way, you'll learn:

- IP basics for writing effective network programs, such as IPv4 and IPv6 multicasting, ports, and network address translation
- How to use handlers, middleware, and multiplexers to build capable HTTP-based applications with minimal code
- The OSI and TCP/IP models for layered data architectures
- Methods for reading data from/writing data to a network connection, like the type-length-value encoding scheme
- Tools for incorporating

authentication and encryption into your applications using TLS, like mutual authentication • How to serialize data for storage or transmission in Go-friendly formats like JSON, Gob, XML, and protocol buffers • How to Leverage Go's code generation support to efficiently communicate with gRPC-based network services So get ready to take advantage of Go's built-in concurrency, rapid compiling, and rich standard library. Because when it comes to writing robust network programs, it's Go time.

"A complete guide to the challenges and solutions in securing microservices architectures." —Massimo Siani, FinDynamic Key Features Secure microservices infrastructure and code Monitoring, access control, and microservice-to-microservice communications Deploy securely using Kubernetes, Docker, and the Istio service mesh. Hands-on examples and exercises using Java and Spring Boot Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. Microservices Security in Action teaches you how to address microservices-specific security challenges throughout the system. This practical guide includes plentiful hands-on exercises using industry-leading open-source tools and examples using Java and Spring Boot. About The Book Design and implement security into your microservices from the start. Microservices Security in Action teaches you to assess and address security challenges at every level of a Microservices application, from APIs to infrastructure. You'll find effective solutions to common security problems, including throttling and monitoring, access control at the API gateway, and microservice-to-microservice communication. Detailed Java code samples, exercises, and real-world business use cases ensure you can put what you've learned into action immediately. What You Will Learn Microservice security concepts Edge services with an API gateway Deployments with Docker, Kubernetes, and Istio Security testing at the code level Communications with HTTP, gRPC, and Kafka This Book Is Written For For experienced microservices developers with intermediate Java skills. About The Author Prabath Siriwardena is the vice president of security architecture at WSO2. Nuwan Dias is the director of API architecture at WSO2. They have designed secure systems for many Fortune 500 companies. Table of Contents PART 1 OVERVIEW 1 Microservices security landscape 2 First steps in securing microservices PART 2 EDGE SECURITY 3 Securing north/south traffic with an API gateway 4 Accessing a secured microservice via a single-page application 5 Engaging throttling, monitoring, and access control PART 3 SERVICE-TO-SERVICE COMMUNICATIONS 6 Securing east/west traffic with certificates 7 Securing east/west traffic with JWT 8 Securing east/west traffic over gRPC 9 Securing reactive microservices PART 4 SECURE DEPLOYMENT 10 Conquering container security with Docker 11 Securing microservices on Kubernetes 12 Securing microservices with Istio service mesh PART 5 SECURE DEVELOPMENT 13 Secure coding practices and automation

The Highlights Book of Things to Do is the essential book of pure creativity and inspiration. Kids ages seven and up will find hundreds of ways to build, play, experiment, craft, cook, dream, think, and become outstanding citizens of the world. This highly visual, hands-on activity book shows kids some of the best ways to do great things--from practicing the lost arts of knot-tying, building campfires, connecting circuits, playing jump rope, drawing maps, and writing letters, to learning how to empower themselves socially, emotionally, and in their communities. The final chapter, Do Great Things, inspires kids become caring individuals, confident problem solvers, and thoughtful people who can change the world. Full List of Chapters: Things to Do Inside Things to Do Outside Science Experiments to Do Things to Build Things to Do with Your Brain Things to Do in the Kitchen Things to Draw Things to Write Things to Do with Color Things to Do with Paper More Things to Do with Recycled Materials Do Great Things National Parenting Seal of Approval Winner, National Parenting Product Award (NAPPA) Winner, Mom's Choice Award, Gold

Security with GoExplore the power of Golang to secure host, web, and cloud servicesPackt Publishing Ltd

This book sheds new light on the important but diverse roles of women in the civil war in Nepal (1996-2006), and the post-conflict reconstruction period (2006-2016). Engaging critically with the women, peace and security literature, Women, Peace and Security in Nepal questions the potential of peace processes to become a window of opportunity for women's empowerment, while insisting on the vital importance of a gender perspective in the study of conflict, security and peace. After the signing of the 2006 Comprehensive Peace Accord, Nepal experienced a huge leap in women's political representation in the subsequent Constituent Assembly, often portrayed as a landmark victory for women's empowerment in the context of South Asia. Nepali women's mobilization played a key role in this success story, though similar mobilization has failed to produce the same outcomes elsewhere in South Asia. How does Nepal differ from the other cases? Presenting studies of war-time and post-conflict Nepal through a gender lens, this book critically assesses the argument that war and peacebuilding can add momentum to the transformation of gender roles. Contributing new knowledge on women's disempowerment and empowerment in conflict and peacebuilding, the book also offers insights for contemporary debate on gender and political change in conflict-affected societies. This book will be of great interest to students of peace and conflict studies, gender security, South Asia and international relations in general, as well as policy-makers and NGOs.

An insightful guide to learning the Go programming language About This Book Get insightful coverage of Go programming syntax, constructs, and idioms to help you understand Go code Get a full explanation of all the known GoF design patterns in Go, including comprehensive theory and examples Learn to apply the nuances of the Go language, and get to know the open source community that surrounds it to implement a wide range of start-up quality projects Who This Book Is For Beginners to Go who are comfortable in other OOP languages like Java, C#, or Python will find this course interesting and beneficial. What You Will Learn Install and configure the Go development environment to quickly get started with your first program Use the basic elements of the language including source code structure, variables, constants, and control flow primitives Get to know all the basic syntax and tools you need to start coding in Go Create unique instances that cannot be duplicated within a program Build quirky and fun projects from scratch while exploring patterns, practices, and techniques, as well as a range of different technologies Create websites and data services capable of massive scaling using Go's net/http package, Explore RESTful patterns as well as low-latency WebSocket APIs Interact with a variety of remote web services to consume capabilities, ranging from authentication and authorization to a fully functioning thesaurus In Detail The Go programming language has firmly established itself as a favorite for building complex and scalable system applications. Go offers a direct and practical approach to programming that lets programmers write correct and predictable code using concurrency idioms and a full-featured standard library. This practical guide is full of real-world examples to help you get started with Go in no time at all. You'll start by understanding the fundamentals of Go, then get a detailed description of the Go data types, program structures, and Maps. After that, you'll learn how to use Go concurrency idioms to avoid pitfalls and create programs that are exact in expected behavior. Next, you will get familiar with the tools and libraries that are available in Go to write and exercise tests, benchmarking, and code coverage. After that, you will be able to utilize some of the most important features of GO such as Network Programming and OS integration to build efficient applications. Then you'll start applying your skills to build some amazing projects in Go. You will learn to develop high-quality command-line tools that utilize the powerful shell capabilities and perform well using Go's built-in concurrency mechanisms. Scale, performance, and high availability lie at the heart of our projects, and the lessons learned throughout the sections will arm you with everything you need to build world-class solutions. You will get a feel for app deployment using Docker and Google App Engine. Each project could form the basis of a start-up, which means they are directly applicable to modern software markets. With these skills in hand, you will be able to conquer all your fears of application development and go on to build large, robust and succinct apps in Go. This Learning Path combines some of the best that Packt has to offer in one complete, curated package. It includes content from the following Packt products: Learning Go Programming Go Design Patterns Go Programming Blueprints, Second Edition Style

and approach Full of real-world, practical examples, this course teaches you the widely used design patterns and best practices in Go in a step-by-step manner. It also provides fun projects that involve building applications from scratch.

The Go Programming Language is the authoritative resource for any programmer who wants to learn Go. It shows how to write clear and idiomatic Go to solve real-world problems. The book does not assume prior knowledge of Go nor experience with any specific language, so you'll find it accessible whether you're most comfortable with JavaScript, Ruby, Python, Java, or C++. The first chapter is a tutorial on the basic concepts of Go, introduced through programs for file I/O and text processing, simple graphics, and web clients and servers. Early chapters cover the structural elements of Go programs: syntax, control flow, data types, and the organization of a program into packages, files, and functions. The examples illustrate many packages from the standard library and show how to create new ones of your own. Later chapters explain the package mechanism in more detail, and how to build, test, and maintain projects using the go tool. The chapters on methods and interfaces introduce Go's unconventional approach to object-oriented programming, in which methods can be declared on any type and interfaces are implicitly satisfied. They explain the key principles of encapsulation, composition, and substitutability using realistic examples. Two chapters on concurrency present in-depth approaches to this increasingly important topic. The first, which covers the basic mechanisms of goroutines and channels, illustrates the style known as communicating sequential processes for which Go is renowned. The second covers more traditional aspects of concurrency with shared variables. These chapters provide a solid foundation for programmers encountering concurrency for the first time. The final two chapters explore lower-level features of Go. One covers the art of metaprogramming using reflection. The other shows how to use the unsafe package to step outside the type system for special situations, and how to use the cgo tool to create Go bindings for C libraries. The book features hundreds of interesting and practical examples of well-written Go code that cover the whole language, its most important packages, and a wide range of applications. Each chapter has exercises to test your understanding and explore extensions and alternatives. Source code is freely available for download from <http://gopl.io/> and may be conveniently fetched, built, and installed using the go get command.

“Original and imaginative . . . Ripping suspense, sheer terror, and a wrenching love story.” —Sandra Brown, New York Times bestselling author of Friction The terrible truth about Manderley is that someone is always watching. Manderley Resort is a gleaming, new twenty-story hotel on the California coast. It's about to open its doors, and the world--at least those with the means to afford it--will be welcomed into a palace of opulence and unparalleled security. But someone is determined that Manderley will never open. The staff has no idea that their every move is being watched, and over the next twelve hours they will be killed off, one by one. Writing in the tradition of Edgar Allan Poe and Stephen King, and with a deep bow to Daphne du Maurier, author Gina Wohlsdorf pairs narrative ingenuity and razor-wire prose with quick twists, sharp turns, and gasp-inducing terror. Security is grand guignol storytelling at its very best. A shocking thriller, a brilliant narrative puzzle, and a multifaceted love story unlike any other, Security marks the debut of a fearless and gifted writer. “Be surprised, be very surprised: Gina Wohlsdorf brings more than just plot twists and a terrifically tender love story to this thriller . . . It's her playful homage to Hitchcock and du Maurier that had me reading, howling, and just plain loving this novel.” —Sara Gruen, author of At the Water's Edge “Grand Hotel meets Psycho in the age of surveillance . . . Security is cinematically vivid, crisply written, and sharp enough to cut . . . Wohlsdorf brilliantly subverts our expectations of the action genre in this smart, shocking, poignant thriller.” —Emily Croy Barker, author of The Thinking Woman's Guide to Real Magic “The thrill of this novel goes beyond its wickedly clever, split-screen, high-tech wizardry—a kind of video gamer's literary retake of Hitchcock's Rear Window--and emanates from its strange, disembodied narrator . . . The effect is terrifying, sexy, dizzying, and impossible to look away from.” —Tim Johnston, author of Descent “Shocking and filled with Tarantino-ish dark humor. . . Structurally reminiscent of the amazing Jennifer Egan, Wohlsdorf's book is certainly a hybrid, like nothing else. Get ready.” —Ann Beattie, author of The State We're In “Flawless . . . Security is perfectly tuned for blockbuster status . . . They don't make a hotel big enough to house all the people who will want to read this, and soon, as in Manderley, all eyes will be on Wohlsdorf.” —Daniel Kraus, Booklist, starred review

Like the best-selling Black Hat Python, Black Hat Go explores the darker side of the popular Go programming language. This collection of short scripts will help you test your systems, build and automate tools to fit your needs, and improve your offensive security skillset. Black Hat Go explores the darker side of Go, the popular programming language revered by hackers for its simplicity, efficiency, and reliability. It provides an arsenal of practical tactics from the perspective of security practitioners and hackers to help you test your systems, build and automate tools to fit your needs, and improve your offensive security skillset, all using the power of Go. You'll begin your journey with a basic overview of Go's syntax and philosophy and then start to explore examples that you can leverage for tool development, including common network protocols like HTTP, DNS, and SMB. You'll then dig into various tactics and problems that penetration testers encounter, addressing things like data pilfering, packet sniffing, and exploit development. You'll create dynamic, pluggable tools before diving into cryptography, attacking Microsoft Windows, and implementing steganography. You'll learn how to:

- Make performant tools that can be used for your own security projects
- Create usable tools that interact with remote APIs
- Scrape arbitrary HTML data
- Use Go's standard package, net/http, for building HTTP servers
- Write your own DNS server and proxy
- Use DNS tunneling to establish a C2 channel out of a restrictive network
- Create a vulnerability fuzzer to discover an application's security weaknesses
- Use plug-ins and extensions to future-proof products

Build an RC2 symmetric-key brute-forcer • Implant data within a Portable Network Graphics (PNG) image. Are you ready to add to your arsenal of security tools? Then let's Go!

Computers at Risk presents a comprehensive agenda for developing nationwide policies and practices for computer security. Specific recommendations are provided for industry and for government agencies engaged in computer security activities. The volume also outlines problems and opportunities in computer security research, recommends ways to improve the research infrastructure, and suggests topics for investigators. The book explores the diversity of the field, the need to engineer countermeasures based on speculation of what experts think computer attackers may do next, why the technology community has failed to respond to the need for enhanced security systems, how innovators could be encouraged to bring more options to the marketplace, and balancing the importance of security against the right of privacy.

This practical, tutorial-style book uses the Kali Linux distribution to teach Linux basics with a focus on how hackers would use them. Topics include Linux command line basics, filesystems, networking, BASH basics, package management, logging, and the Linux kernel and drivers. If you're getting started along the exciting path of hacking, cybersecurity, and pentesting, Linux Basics for Hackers is an excellent first step. Using Kali Linux, an advanced penetration testing distribution of Linux, you'll learn the basics of using the Linux operating system and acquire the tools and techniques you'll need to take control of a Linux environment. First, you'll learn how to install Kali on a virtual machine and get an introduction to basic Linux concepts. Next, you'll tackle broader Linux topics like manipulating text, controlling file and directory permissions, and managing user environment variables. You'll then focus in on foundational hacking concepts like security and anonymity and learn scripting skills with bash and Python. Practical tutorials and exercises throughout will reinforce and test your skills as you learn how to:

- Cover your tracks by changing your network information and manipulating the rsyslog logging utility
- Write a tool to scan for network connections, and connect and listen to wireless networks
- Keep your internet activity stealthy using Tor, proxy servers, VPNs, and encrypted email
- Write a bash script to scan open ports for potential targets
- Use and abuse services like MySQL, Apache web

server, and OpenSSH - Build your own hacking tools, such as a remote video spy camera and a password cracker Hacking is complex, and there is no single way in. Why not start at the beginning with Linux Basics for Hackers?

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.

This anniversary edition which has stood the test of time as a runaway best-seller provides a practical, straight-forward guide to achieving security throughout computer networks. No theory, no math, no fiction of what should be working but isn't, just the facts. Known as the master of cryptography, Schneier uses his extensive field experience with his own clients to dispel the myths that often mislead IT managers as they try to build secure systems. A much-touted section: Schneier's tutorial on just what cryptography (a subset of computer security) can and cannot do for them, has received far-reaching praise from both the technical and business community. Praise for Secrets and Lies "This is a business issue, not a technical one, and executives can no longer leave such decisions to techies. That's why Secrets and Lies belongs in every manager's library."-Business Week "Startlingly lively....a jewel box of little surprises you can actually use."-Fortune "Secrets is a comprehensive, well-written work on a topic few business leaders can afford to neglect."-Business 2.0 "Instead of talking algorithms to geeky programmers, [Schneier] offers a primer in practical computer security aimed at those shopping, communicating or doing business online-almost everyone, in other words."-The Economist "Schneier...peppers the book with lively anecdotes and aphorisms, making it unusually accessible."-Los Angeles Times With a new and compelling Introduction by the author, this premium edition will become a keepsake for security enthusiasts of every stripe.

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.

[Copyright: a927857a5a7e432fb25409d7dec23d5e](#)