Computer Security 3rd Edition Dieter Gollmann

"This book provides a valuable resource by addressing the most pressing issues facing cyber-security from both a national and global perspective"--Provided by publisher.
Take on the perspective of an attacker with this insightful new resource for ethical hackers, pentesters, and social engineers In The Art of Attack: Attacker Mindset for Security Professionals, experienced physical pentester and social engineer Maxie Reynolds untangles the threads of a useful, sometimes dangerous, mentality. The book shows ethical hackers, social engineers, and pentesters what an attacker mindset is and how to and how to use it to their advantage. Adopting this mindset will result in the improvement of security, offensively and defensively, by allowing you to see your environment objectively through the eyes of an attacker. The book shows you the laws of the mindset and the techniques attackers use, from persistence to “start with the end” strategies and non-linear thinking, that make them so dangerous. You’ll discover: A variety of attacker strategies, including approaches, processes, reconnaissance, privilege escalation, redundant access, and escape techniques The unique tells and signs of an attack and how to avoid becoming a victim of one What the science of psychology tells us about amygdala hijacking and other tendencies that you need to protect against Perfect for red teams, social engineers, pentesters, and ethical hackers seeking to fortify and harden their systems and the systems of their clients, The Art of Attack is an invaluable resource for anyone in the technology security space seeking a one-stop resource that puts them in the mind of an attacker.
Insider Threats in Cyber Security is a cutting edge text presenting IT and non-IT facets of insider threats together. This volume brings together a critical mass of well-established worldwide researchers, and provides a unique multidisciplinary overview. Monica van Huystee, Senior Policy Advisor at MCI, Ontario, Canada comments "The book will be a must read, so of course I’ll need a copy." Insider Threats in Cyber Security covers all aspects of insider threats, from motivation to mitigation. It includes how to monitor insider threats (and what to monitor for), how to mitigate insider threats, and related topics and case studies. Insider Threats in Cyber Security is intended for a professional audience composed of the military, government policy makers and banking; financing companies focusing on the Secure Cyberspace industry. This book is also suitable for advanced-level students and researchers in computer science as a secondary text or reference book.
A completely up-to-date resource on computer security Assuming no previous experience in the field of computer security, this must-have book walks you through the many essential aspects of this vast topic, from the newest advances in software and technology to the most recent information on Web applications security. This new edition includes sections on Windows NT, CORBA, and Java and discusses cross-site scripting and JavaScript hacking as well as SQL injection. Serving as a helpful introduction, this self-study guide is a wonderful starting point for examining the variety of competing security systems and what makes them different from one another. Unravels the complex topic of computer security and breaks it down in such a way as to serve as an ideal introduction for beginners in the field of computer security Examines the foundations of computer security and its basic principles Addresses username and password, password protection, single sign-on, and more Discusses operating system

integrity, hardware security features, and memory Covers Unix security, Windows security, database security, network security, web security, and software security Packed with in-depth coverage, this resource spares no details when it comes to the critical topic of computer security.

This is the third edition of this influential and comprehensive handbook. Substantive changes in international humanitarian law have taken place recently, including a progressive development of customary law; and the jurisprudence of national courts, international ad hoc tribunals and theInternational Criminal Court, which have made a reassessment of this vitally important part of international law both timely and topical.New material is extensively incorporated, including new developments in treaty law, such as the 2010 amendments to the ICC Statute, as well as new topics that have been extensively debated in recent years: direct participation in hostilities; air and missile warfare; belligerent occupation;operational detention; and the protection of the environment in armed conflict. The growing need to consider borderline issues of the law of armed conflict and the interplay of international humanitarian law, human rights, and other branches of international law have led to have led to some materialbeing considered in a new light.The commentary both deepens reflection on such innovations, and critically reconsiders views expressed in earlier editions to provide a contemporary analysis of this changing field. Renowned international lawyers offer a broad spectrum of legal opinions, restating the law in this area, which isapplicable worldwide. Issues of human rights in armed conflicts and in post-conflict situations are extensively addressed. Controversial opinions and national and international judgments are documented and discussed. Problems of application of the law in recent military campaigns are assessed andinterpreted in a practice-oriented manner. Based on best-practice rules of global importance, this book also sets out an international 'manual' for international humanitarian law in armed conflicts.

Network Security Essentials, Third Edition is a thorough, up-to-date introduction to the deterrence, prevention, detection, and correction of security violations involving information delivery across networks and the Internet.

This introduction to first-order logic clearly works out the role of first-order logic in the foundations of mathematics, particularly the two basic questions of the range of the axiomatic method and of theorem-proving by machines. It covers several advanced topics not commonly treated in introductory texts, such as Fraïssé's characterization of elementary equivalence, Lindström's theorem on the maximality of first-order logic, and the fundamentals of logic programming.

Shows chronic dieters how to restore their intuition about how much food their body needs, how to rediscover the delights of food, how to lose weight naturally, and how to discover their natural weight. Tour.

Presents an introduction to the open-source electronics prototyping platform.

This book covers the fundamental principles in Computer Security. Via hands-on activities, the book aims to help readers understand the risks with software application and computer system, how various attacks work, what their fundamental causes are, how the countermeasures work, and how to defend against them in programs and systems.

The fourth edition of the Handbook of Human Factors and Ergonomicshas been completely revised and updated. This includes allexisting third edition chapters plus new chapters written to covernew areas. These include the following subjects: Managing low-back disorder risk in the workplace Online interactivity Neuroergonomics Office ergonomics Social networking

HF&E in motor vehicle transportation User requirements Human factors and ergonomics in aviation Human factors in ambient intelligent environments As with the earlier editions, the main purpose of this handbookis to serve the needs of the human factors and ergonomicsresearchers, practitioners, and graduate students. Each chapter hasa strong theory and scientific base, but is heavily focused on realworld applications. As such, a significant number of case studies,examples, figures, and tables are included to aid in theunderstanding and application of the material covered.

This book focuses on technical safety, means of expanding the current procedures, and making the related risks more predictable. It identifies the ‘hidden commonalities’ of the various technical safety concepts and formulates a corresponding procedure, applicable across disciplines, in a single guideline. The future is now: we constantly face change through science, research and technologies, change through industrial development, and new innovations and complexities. Our society fundamentally depends on technical systems, infrastructures and interconnected smart components, in every corner of the human environment. And these systems bring with them the need for technical safety. The risks of extending what is technically feasible have to be identified and analyzed at an early stage so as to avoid and/or mitigate potential harm by means of appropriate countermeasures. Every technical field interprets technical safety in its own way. However, if a safety concept is to be comprehensively applied, it must be compatible with all technical fields – a challenge this book successfully addresses.

This book discusses the current research concerning public key cryptosystems. It begins with an introduction to the basic concepts of multivariate cryptography and the history of this field. The authors provide a detailed description and security analysis of the most important multivariate public key schemes, including the four multivariate signature schemes participating as second round candidates in the NIST standardization process for post-quantum cryptosystems. Furthermore, this book covers the Simple Matrix encryption scheme, which is currently the most promising multivariate public key encryption scheme. This book also covers the current state of security analysis methods for Multivariate Public Key Cryptosystems including the algorithms and theory of solving systems of multivariate polynomial equations over finite fields. Through the book's website, interested readers can find source code to the algorithms handled in this book. In 1994, Dr. Peter Shor from Bell Laboratories proposed a quantum algorithm solving the Integer Factorization and the Discrete Logarithm problem in polynomial time, thus making all of the currently used public key cryptosystems, such as RSA and ECC insecure. Therefore, there is an urgent need for alternative public key schemes which are resistant against quantum computer attacks. Researchers worldwide, as well as companies and governmental organizations have put a tremendous effort into the development of post-quantum public key cryptosystems to meet this challenge. One of the most promising candidates for this are Multivariate Public Key Cryptosystems (MPKCs). The public key of an MPKC is a set of multivariate polynomials over a small finite field. Especially for digital signatures, numerous well-studied multivariate schemes offering very short signatures and high efficiency exist. The fact that these schemes work over small finite fields, makes them suitable not only for interconnected computer systems, but also for small devices with limited resources, which are used in ubiquitous computing. This book gives a systematic introduction into the field of Multivariate Public Key Cryptosystems (MPKC), and presents the most promising multivariate schemes for digital signatures and encryption. Although, this book was written more from a computational perspective, the authors try to provide the necessary mathematical background. Therefore, this book is suitable for a broad audience. This would include researchers working in either computer science or mathematics interested in this exciting new field, or as a secondary textbook for a course in MPKC suitable for beginning graduate students in mathematics or computer science. Information security experts in industry, computer scientists and mathematicians would also find this book valuable as a guide for understanding the basic mathematical structures necessary to implement multivariate cryptosystems for practical applications

Written by experienced experts in molecular modeling, this books describes the basics to the extent that is necessary if one wants to be able to reliably judge the results from molecular modeling calculations. Its main objective is the description of the various pitfalls to be avoided. Without unnecessary overhead it leads the reader from simple calculations on small molecules to the modeling of proteins and other relevant biomolecules. A textbook for beginners as well as an invaluable reference for all those dealing with molecular modeling in their daily work!

Natural capital is what nature provides to us for free. Renewables—like species—keep on coming, provided we do not drive them towards extinction. Non-renewables—like oil and gas—can only be used once. Together, they are the foundation that ensures our survival and well-being, and the basis of all economic activity. In the face of the global, local, and national destruction of biodiversity and ecosystems, economist Dieter Helm here offers a crucial set of strategies for establishing natural capital policy that is balanced, economically sustainable, and politically viable. Helm shows why the commonly held view that environmental protection poses obstacles to economic progress is false, and he explains why the environment must be at the very core of economic planning. He presents the first real attempt to calibrate, measure, and value natural capital from an economic perspective and goes on to outline a stable new framework for sustainable growth. Bristling with ideas of immediate global relevance, Helm’s book shifts the parameters of current environmental debate. As inspiring as his trailblazing The Carbon Crunch, this volume will be essential reading for anyone concerned with reversing the headlong destruction of our environment.

This book, written by leaders in the protection field of critical infrastructures, provides an extended overview of the technological and operative advantages together with the security problems and challenges of the new paradigm of the Internet of Things in today’s industry, also known as the Industry Internet of Things (IIoT). The incorporation of the new embedded technologies and the interconnected networking advances in the automation and monitoring processes, certainly multiplies the functional complexities of the underlying control system, whilst increasing security and privacy risks. The critical nature of the application context and its relevance for the well-being of citizens and their economy, attracts the attention of multiple, advanced attackers, with stealthy abilities to evade security policies, ex-filter information or exploit vulnerabilities. Some real-life events and registers in CERTs have already clearly demonstrated how the control industry can become vulnerable to multiple types of advanced threats whose focus consists in hitting the safety and security of the control processes. This book, therefore, comprises a detailed spectrum of research papers with highly analytical content and actuation procedures to cover the relevant security and privacy issues such as data protection, awareness, response and resilience, all of them working at optimal times. Readers will be able to comprehend the construction problems of the fourth industrial revolution and are introduced to effective, lightweight protection solutions which can be integrated as part of the new IIoT-based monitoring ecosystem.

Featuring foldouts, candid photographs, and full-page color installation shots, this beautiful new book celebrates the work of Jean-Michel Basquiat over his brief but meteoric career. Dozens of historical photographs, both black-and-white and color, connect the text with the close to sixty color plates, providing invaluable insight into the life and work of this seminal artist. Art historian Robert Farris Thompson delivers a detailed analysis of some of Basquiat’s most iconic paintings, situating them within the artist’s own oeuvre, as well as the larger landscape of twentieth-century art. Rounding out this stunning volume, the late Rene Ricard provides a rare but accurate glimpse into the private world of Basquiat, recounting their sometimes fraught friendship, from their first meeting in 1981 to Basquiat's death in 1988.

This open access book presents a topical, comprehensive and differentiated analysis of Germany's public administration and reforms. It provides an overview on key elements of German public administration at the federal, Länder and local levels of government as well as on current reform activities of the public sector. It examines the key institutional features of German public administration; the changing relationships between public administration, society and the private sector; the administrative reforms at different levels of the federal system and numerous sectors; and new challenges and modernization approaches like digitalization, Open Government and Better Regulation. Each chapter offers a combination of descriptive information and problem-oriented analysis, presenting key topical issues in Germany which are relevant to an international readership.

This book constitutes the refereed proceedings of the 22nd International Conference on Information and Communications Security, ICICS 2020, held in Copenhagen, Denmark*, in August 2020. The 33 revised full papers were carefully selected from 139 submissions. The papers focus in topics about computer and communication security, and are organized in topics of security and cryptography. *The conference was held virtually due to the COVID-19 pandemic.

Presents theories and models associated with information privacy and safeguard practices to help anchor and guide the development of technologies, standards, and best practices. Provides recent, comprehensive coverage of all issues related to information security and ethics, as well as the opportunities, future challenges, and emerging trends related to this subject.

This volume constitutes the proceedings of the Third European Symposium on Research in Computer Security, held in Brighton, UK in November 1994. The 26 papers presented in the book in revised versions were carefully selected from a total of 79 submissions; they cover many current aspects of computer security research and advanced applications. The papers are grouped in sections on high security assurance software, key management, authentication, digital payment, distributed systems, access control, databases, and measures.

This is the 70th encyclopaedia of library and information science. It covers topics such as: intelligent systems for problem analysis in organizations; interactive system design; international models of school library development; lexicalization in natural language generation; and more.

A must for working network and security professionals as well as anyone in IS seeking to build competence in the increasingly important field of security Written by three high-profile experts, including Eric Cole, an ex-CIA security guru who appears regularly on CNN and elsewhere in the media, and Ronald Krutz, a security pioneer who cowrote The CISSP Prep Guide and other security bestsellers Covers everything from basic security principles and practices to the latest security threats and responses, including proven methods for diagnosing network vulnerabilities and insider secrets for boosting security effectiveness

Augmented reality (AR) is one of today's most fascinating and future-oriented areas of computer science and technology. By overlaying computer-generated information on views of the real world, AR amplifies human perception and cognition in remarkable new ways. Do you like the virtual first-down line in football games on TV? That's AR. And AR apps are rapidly coming to billions of smartphones, too. Working in AR requires knowledge from diverse disciplines, including computer vision, computer graphics, and human-computer interaction (HCI). Augmented Reality: Principles and Practice integrates all this knowledge into a single-source reference, presenting the most significant AR work with scrupulous accuracy. Dieter Schmalstieg, a pioneer of both AR foundation and application, is drawing from his two decades of AR experience to clearly present the field. Together with mobile AR pioneer and research colleague Tobias Höllerer, the authors address all aspects of the field, illuminating AR from both technical and HCI perspectives. The authors review AR's technical foundations, including display and tracking technologies, show how AR emerges from the symbiosis of computer vision and computer graphics, introduce AR-specific visualization and 3D interaction techniques, and showcase applications from diverse industries. They conclude with an outlook on trends and emerging technologies, including practical pointers for beginning practitioners. This book is an indispensable resource for everyone interested in AR, including software and app developers, engineers, students and instructors, researchers, and hobbyists. For use in educational environments, the authors will provide a companion website containing slides, code examples, and other source materials.

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.

Now that there’s software in everything, how can you make anything secure? Understand how to engineer dependable systems with this newly updated classic In Security Engineering: A Guide to Building Dependable Distributed Systems, Third Edition Cambridge University professor Ross Anderson updates his classic textbook and teaches readers how to design, implement, and test systems to withstand both error and attack. This book became a best-seller in 2001 and helped establish the discipline of security engineering. By the second edition in 2008, underground dark markets had let the bad guys specialize and scale up; attacks were increasingly on users rather than on technology. The book repeated its success by showing how security engineers can focus on usability. Now the third edition brings it up to date for 2020. As people now go online from phones more than laptops, most servers are in the cloud, online advertising drives the Internet and social networks have taken over much human interaction, many patterns of crime and abuse are the same, but the methods have evolved. Ross Anderson explores what security engineering means in 2020, including: How the basic elements of cryptography, protocols, and access control translate to the new world of phones, cloud services, social media and the Internet of Things Who the attackers are – from nation states and business competitors through criminal gangs to stalkers and playground bullies What they do – from phishing and carding through SIM swapping and software exploits to DDoS and fake news Security psychology, from privacy through ease-of-use to deception The economics of security and dependability – why companies build vulnerable systems and governments look the other way How dozens of industries went online – well or badly How to manage security and safety engineering in a world of agile development – from reliability engineering to DevSecOps The third edition of Security Engineering ends with a grand challenge: sustainable security. As we build ever more software and connectivity into safety-critical durable goods like cars and medical devices, how do we design systems we can maintain and defend for decades? Or will everything in the world need monthly software upgrades, and become unsafe once they stop?

This book constitutes the revised refereed summary of the results presented during the European IST/FET proactive initiative's Global Computing workshop, GC 2003, held in Rovereto, Italy, in February 2003. The eight revised full papers and survey articles presented together with a detailed introductory overview assess the state of the art in global computing. Global computing attempts to develop models, frameworks, methods, and algorithms to build systems that are flexible, dependable, secure, robust, and efficient. The dominant technical issues are coordination, interaction, security, safety, scalability, robustness, mobility, risk management, performance analysis, etc.

It is August 2020 as President Donald Trump’s loyal supporters pack into election rallies, blatantly ignoring the global pandemic raging around them. With the nation still deeply divided over many issues that include lockdowns, masks, and personal freedoms, three couples meet to discuss the pandemic. They have their own ideas and facts to back them up on how to best handle the current challenges facing the United States. While humanity deals with the virus in a variety of ways, civil rights protests erupt as scientists doggedly work to develop a vaccine. When a new president is elected, armed demonstrators storm the US Capitol. But what no one knows is that deadly mutations are lurking in the shadows, just waiting to wreak more havoc onto the world. With many parents dying or dead, small children cry and wander the streets looking for help. How will they cope? Pandemic is a thrilling tale that follows the catastrophic events surrounding the COVID-19 pandemic and unrest in a nation deeply divided both before and after the presidential election.

This reference guide to creating high quality security software covers the complete suite of security applications referred to as end2end security. It illustrates basic concepts of security engineering through real-world examples.

The Growing Imperative Need for Effective Information Security Governance With monotonous regularity, headlines announce ever more spectacular failures of information security and mounting losses. The succession of corporate debacles and dramatic control failures in recent years underscores the necessity for information security to be tightly integrated into the fabric of every organization. The protection of an organization's most valuable asset information can no longer be relegated to low-level technical personnel, but must be considered an essential element of corporate governance that is critical to organizational success and survival. Written by an industry expert, Information Security Governance is the first book-length treatment of this important topic, providing readers with a step-by-step approach to developing and managing an effective information security program. Beginning with a general overview of governance, the book covers: The business case for information security Defining roles and responsibilities Developing strategic metrics Determining information security outcomes Setting security governance objectives Establishing risk management objectives Developing a cost-effective security strategy A sample strategy development The steps for implementing an effective strategy Developing meaningful security program development metrics Designing relevant information security management metrics Defining incident management and response metrics Complemented with action plans and sample policies that demonstrate to readers how to put these ideas into practice, Information Security Governance is indispensable reading for any professional who is involved in information security and assurance.

Quality of Protection: Security Measurements and Metrics is an edited volume based on the Quality of Protection Workshop in Milano, Italy (September 2005). This volume discusses how security research can progress towards quality of protection in security comparable to quality of service in networking and software measurements, and metrics in empirical software engineering. Information security in the business setting has matured in the last few decades. Standards such as IS017799, the Common Criteria (ISO15408), and a number of industry certifications and risk analysis methodologies have raised the bar for good security solutions from a business perspective. Designed for a professional audience composed of researchers and practitioners in industry, Quality of Protection: Security Measurements and Metrics is also suitable for advanced-level students in computer science.

This book constitutes the refereed proceedings of the 8th European Symposium on Research in Computer Security, ESORICS 2003, held in Gjovik, Norway in October 2003. The 19 revised full papers presented were carefully reviewed and selected from 114 submissions. Among the topics addressed are signature control, access control, key exchange, broadcast protocols, privacy preserving technologies, attack analysis, electronic voting, identity control, authentication, security services, smart card security, formal security protocols analysis, and intrusion detection.

Computer Security, Second Edition offers security newcomers a grounding in the basic principles involved in preventing security breaches and protecting electronic data. It outlines security strategies to counter problems that will be faced in UNIX and Windows NT operating systems, distributed systems, the Web, and object-oriented systems.

This book serves as both a textbook and handbook on the benchmarking of systems and components used as building blocks of modern information and communication technology applications. It provides theoretical and practical foundations as well as an in-depth exploration of modern benchmarks and benchmark development. The book is divided into two parts: foundations and applications. The first part introduces the foundations of benchmarking as a discipline, covering the three fundamental elements of each benchmarking approach: metrics, workloads, and measurement methodology. The second part focuses on different application areas, presenting contributions in specific fields of benchmark development. These contributions address the unique challenges that arise in the conception and development of benchmarks for specific systems or subsystems, and demonstrate how the foundations and concepts in the first part of the book are being used in existing benchmarks. Further, the book presents a number of concrete applications and case studies based on input from leading benchmark developers from consortia such as the Standard Performance Evaluation Corporation (SPEC) and the Transaction Processing Performance Council (TPC). Providing both practical and theoretical foundations, as well as a detailed discussion of modern benchmarks and their development, the book is intended as a handbook for professionals and researchers working in areas related to benchmarking. It offers an up-to-date point of reference for existing work as well as latest results, research challenges, and future research directions. It also can be used as a textbook for graduate and postgraduate students studying any of the many subjects related to benchmarking. While readers are assumed to be familiar with the principles and practices of computer science, as well as software and systems engineering, no specific expertise in any subfield of these disciplines is required.

The first book to introduce computer architecture for security and provide the tools to implement secure computer systems This book provides the fundamentals of computer architecture for security. It covers a wide range of computer hardware, system software and data concepts from a security perspective. It is essential for computer science and security professionals to understand both hardware and software security solutions to survive in the workplace. Examination of memory, CPU architecture and system implementation Discussion of computer buses and a dual-port bus interface Examples cover a board spectrum of hardware and software systems Design and implementation of a patent-pending secure computer system Includes the latest patent-pending technologies in architecture security Placement of computers in a security fulfilled network environment Co-authored by the inventor of the modern Computed Tomography (CT) scanner Provides website for lecture notes, security tools and latest updates

This Festschrift was published in honor of Egon Börger on the occasion of his 75th birthday. It acknowledges Prof. Börger's inspiration as a scientist, author, mentor, and community organizer. Dedicated to a pioneer in the fields of logic and computer science, Egon Börger's research interests are unusual in scope, from programming languages to hardware architectures, software architectures, control systems, workflow and interaction patterns, business processes, web applications, and concurrent systems. The 18 invited contributions in this volume are by leading researchers in the areas of software engineering, programming languages, business information systems, and computer science logic.

This long-awaited new edition has been fully updated and revised by the original authors as well as two new members of the author team. Based on many years of active research and teaching it takes the discipline's most difficult aspects and makes them accessible and interesting. Each chapter builds up an understanding of the different ways of looking at the world. The clarity of presentation allows students to rapidly develop a theoretical framework and to apply this knowledge widely as a way of understanding both more advanced theoretical texts and events in world politics. Suitable for first and second year undergraduates studying international relations and international relations theory.