The Cuckoos Egg Tracking A Spy Through The Maze Of Computer Espionage

For more than 40 years, Computerworld has been the leading source of technology news and information for IT influencers worldwide. Computerworld's award-winning Web site (Computerworld.com), twice-monthly publication, focused conference series and custom research form the hub of the world's largest global IT media network.

The Cuckoo's EggTracking a Spy Through the Maze of Computer EspionageSimon and Schuster

Cybercrime focuses on the growing concern about the use of electronic communication for criminal activities and the appropriateness of the countermeasures that are being adopted by law enforcement agencies, security services and legislators to address such anxieties. Fuelled by sensational media headlines and news coverage which has done much to encourage the belief that technologies like the Internet are likely to lead to a lawless electronic frontier, Cybercrime provides a more considered and balanced perspective on what is an important and contested arena for debate. It looks at: *legislation *electronic criminal behaviour *privacy and liberty *the dangers of surveillance. Cybercrime explains the basic issues surrounding cybercrime and its impact on society.

* Looks at the Internet from a morbid, sordid, entertaining perspective rather than a technical how-to perspective * Makes the Internet fun, fascinating, and non-intimidating for casual users. * Focuses on well-known actors, politicians, performing artists, and other public figures and how they have been treated online.

"This volume looks at the challenges of cyberspace in an interdependent world and at the need for new, cooperative modes of governance to build cyber security. Making networks and critical infrastructure secure requires competent domestic strategies. But it also requires a willingness among governments to take the lead in supporting one another through effective legal structures and agreements such as the Council of Europe Convention on Cybercrime. The authors explore informal and formal bilateral and multilateral approaches to transnational cooperation on cyber security and examine the elements needed for success."--BOOK JACKET.

CD-ROM contains: security tools developed by author; publicly available security tools; modified version of popclient; author's GPG 1.0.1 public key.

Fourth Edition (Traditional Chinese Translation) Sheds New Light on Open Source Intelligence Collection and Analysis. Author Michael Bazzell has been well known and respected in government circles for his ability to locate personal information about any target through Open Source Intelligence (OSINT). In this book, he shares his methods in great detail. Each step of his process is explained throughout sixteen chapters of specialized websites, application programming interfaces, and software solutions. Based on his live and online

video training at IntelTechniques.com, over 250 resources are identified with narrative tutorials and screen captures. This book will serve as a reference guide for anyone that is responsible for the collection of online content. It is written in a hands-on style that encourages the reader to execute the tutorials as they go. The search techniques offered will inspire analysts to "think outside the box" when scouring the internet for personal information. Much of the content of this book has never been discussed in any publication. Always thinking like a hacker, the author has identified new ways to use various technologies for an unintended purpose. This book will improve anyone's online investigative skills. Among other techniques, you will learn how to locate: Hidden Social Network Content Cell Phone Owner Information Twitter GPS & Account Data Hidden Photo GPS & Metadata Deleted Websites & Posts Website Owner Information Alias Social Network Profiles Additional User Accounts Sensitive Documents & Photos Live Streaming Social Content IP Addresses of Users Newspaper Archives & Scans Social Content by Location Private Email Addresses Hidden Personal Videos Duplicate Copies of Photos Personal Radio Communications Compromised Email Information Wireless Routers by Location Hidden Mapping Applications Complete Facebook Data Free Investigative Software Alternative Search Engines Mobile App Network Data Unlisted Addresses Unlisted Phone Numbers Useful Browser Extensions Public Government Records Document Metadata Rental Vehicle Contracts Online Criminal Activity

These authors are both well-known senior researchers at AT&T Bell Labs, and this book is based on their actual experiences maintaining, improving, and redesigning AT&T's Internet gateway. They show why the most popular technologies for keeping intruders out are insufficient, while providing a step-by-step guide to their solution--building firewall gateways.

This Brief presents the overarching framework in which each nation is developing its own cyber-security policy, and the unique position adopted by France. Modern informational crises have penetrated most societal arenas, from healthcare, politics, economics to the conduct of business and welfare. Witnessing a convergence between information warfare and the use of “fake news”, info-destabilization, cognitive warfare and cyberwar, this book brings a unique perspective on modern cyberwarfare campaigns, escalation and de-escalation of cyber-conflicts. As organizations are more and more dependent on information for the continuity and stability of their operations, they also become more vulnerable to cyber-destabilization, either genuine, or deliberate for the purpose of gaining geopolitical advantage, waging wars, conducting intellectual theft and a wide range of crimes. Subsequently, the regulation of cyberspace has grown into an international effort where public, private and sovereign interests often collide. By analyzing the particular case of France national strategy and capabilities, the authors investigate the difficulty of obtaining a global agreement on the regulation of cyber-warfare. A review of the motives for disagreement between parties suggests that the current regulation framework is not adapted to the current technological change in the cybersecurity domain. This book suggests a paradigm shift in handling and anchoring cyber-regulation into a new realm of behavioral and cognitive sciences, and their application to machine learning and cyber-defense.

Traditional Chinese Edition of [Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers]

This new Springer volume provides a comprehensive and detailed look at current approaches

to automated question answering. The level of presentation is suitable for newcomers to the field as well as for professionals wishing to study this area and/or to build practical QA systems. The book can serve as a "how-to" handbook for IT practitioners and system developers. It can also be used to teach graduate courses in Computer Science, Information Science and related disciplines.

The rapid evolution of technology continuously changes the way people interact, work, and learn. By examining these advances from a sociological perspective, researchers can further understand the impact of cyberspace on human behavior, interaction, and cognition. Multigenerational Online Behavior and Media Use: Concepts, Methodologies, Tools, and Applications is a vital reference source covering the impact of social networking platforms on a variety of relationships, including those between individuals, governments, citizens, businesses, and consumers. The publication also highlights the negative behavioral, physical, and mental effects of increased online usage and screen time such as mental health issues, internet addiction, and body image. Showcasing a range of topics including online dating, smartphone dependency, and cyberbullying, this multi-volume book is ideally designed for sociologists, psychologists, computer scientists, engineers, communication specialists, academicians, researchers, and graduate-level students seeking current research on media usage and its behavioral effects.

Calder provides an annotated bibliography of scholarly journal material on intelligence, espionage, and related topics selected from vetted articles in fields such as history, criminal justice, political science, military and intelligence studies, humanities, law, and physics from 1844 onward. It contains more than 10,000 citations organized by author, with an extensive key word or term index and an index of coauthors.

The first true account of computer espionage tells of a year-long single-handed hunt for a computer thief who sold information from American computer files to Soviet intelligence agents

In this book, we have hand-picked the most sophisticated, unanticipated, absorbing (if not at times crackpot!), original and musing book reviews of "The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage." Don't say we didn't warn you: these reviews are known to shock with their unconventionality or intimacy. Some may be startled by their biting sincerity; others may be spellbound by their unbridled flights of fantasy. Don't buy this book if: 1. You don't have nerves of steel. 2. You expect to get pregnant in the next five minutes. 3. You've heard it all.

Meet the world's top ethical hackers and explore the tools of the trade Hacking the Hacker takes you inside the world of cybersecurity to show you what goes on behind the scenes, and introduces you to the men and women on the front lines of this technological arms race. Twenty-six of the world's top white hat hackers, security researchers, writers, and leaders, describe what they do and why, with each profile preceded by a no-experience-necessary explanation of the relevant technology. Dorothy Denning discusses advanced persistent threats, Martin Hellman describes how he helped invent public key encryption, Bill Cheswick talks about firewalls, Dr. Charlie Miller talks about hacking cars, and other cybersecurity experts from around the world detail the threats, their defenses, and the tools and techniques they use to thwart the most advanced criminals history has ever seen. Light on jargon and heavy on intrigue, this book is designed to be an introduction to the field; final chapters include a guide for parents of young hackers, as well as the Code of Ethical Hacking to help you start your own journey to the top. Cybersecurity is becoming increasingly critical at all levels, from retail businesses all the way up to national security. This book drives to the heart of the field, introducing the people and practices that help keep our world secure. Go deep into the world of white hat hacking to grasp just how critical cybersecurity is Read the stories of some of the world's most renowned computer security experts Learn how hackers do what they do—no technical expertise necessary Delve into social engineering, cryptography, penetration testing,

network attacks, and more As a field, cybersecurity is large and multi-faceted—yet not historically diverse. With a massive demand for qualified professional that is only going to grow, opportunities are endless. Hacking the Hacker shows you why you should give the field a closer look.

In the early 1990s, people predicted the death of privacy, an end to the current concept of 'property, ' a paperless society, 500 channels of high-definition interactive television, world peace, and the extinction of the human race after a takeover engineered by intelligent machines. Imagining the Internet zeroes in on predictions about the Internet's future and revisits past predictions--and how they turned out. It gives the history of communications in a nutshell, illustrating the serious impact of pervasive networks and how they will change our lives over the next century.

??????????????????????,????????????,??????????????????

"This book reviews problems, issues, and presentations of the newest research in the field of cyberwarfare and cyberterrorism. While enormous efficiencies have been gained as a result of computers and telecommunications technologies, use of these systems and networks translates into a major concentration of information resources, createing a vulnerability to a host of attacks and exploitations"--Provided by publisher.

This is the first complete introduction to and analysis of the politics of the internet. Chapters are arranged around key words and use case studies to guide the reader through a wealth of material. Cyberpower presents all the key concepts of cyberspace including: * power and cyberspace * the virtual individual * society in cyberspace * imagination and the internet.

??????????????,??????????????????????????????,????????????????????????,??????,??????????????????????,?????????,???????????

Traditional Chinese edition of The Greatest Generation

Argues that students are missing out on learning fundamental skills because of the emphasis on becoming computer literate.

Cyberwarfare: Information Operations in a Connected World puts students on the real-world battlefield of cyberspace! It reviews the role that cyberwarfare plays in modern military operations–operations in which it has become almost impossible to separate cyberwarfare from traditional warfare.

The main objective of this book is to explore the concept of cybersecurity in parallel and distributed computing along with recent research developments in the field. It also includes various real-time/offline applications and case studies in the fields of engineering and computer science and the modern tools and technologies used. Information on cybersecurity technologies is organized in the fifteen chapters of this book. This important book cover subjects such as: Research and solutions for the problem of hidden image detection Security aspects of data mining and possible solution techniques A comparative analysis of various methods used in e-commerce security and how to perform secure payment transactions in an efficient manner Blockchain technology and how it is crucial to the security industry Security for the Internet of Things Security issues and challenges in distributed computing security such as heterogeneous computing, cloud computing, fog computing, etc. Demonstrates the administration task issue in unified cloud situations as a multi-target enhancement issue in light of security Explores the concepts of cybercrime and cybersecurity and presents the statistical impact it is having on organizations Highlights some strategies for maintaining the privacy, integrity, confidentiality and availability of cyber information and its real-world impacts such as mobile security software for secure email and online banking, cyber health check programs for business, cyber incident response management, cybersecurity risk management Security policies and mechanisms, various categories of attacks (e.g., denial-of-service), global security architecture, along with distribution of security mechanisms Security issues in the healthcare sector with existing solutions and emerging threats.

If your company or your clients have any presence on the Internet, Digital Communications Law (Revised Edition of former Law and the Information Superhighway) is a must-have resource. This complete compendium helps you handle all Internet-related legal issuesand—from questions of liability connected to sales and communications on the Web, to issues of taxation, to problems that you never thought youand'd faceand—until youand're faced with them! Digital Communications Law is the single, thorough reference that covers all the various laws that affect sales and communications on the Web, including: Liability for harmful communication Taxation Privacy Copyright Trademark Patent Civil litigation Criminal prosecution Constitutional considerations Legal issues in international communication and cross-border commerce As technology advances, Digital Communications Law will keep you current with the laws that arise out of and affect new developments, including disputes and liability connected with: Texting Tweeting Facebook and other social networking sites Net neutrality Dissemination of commercial music and video Advertising Consumer fraud Interoperability and compatibility Accessibility of public information And more!

The prominence and growing dependency on information communication technologies in nearly every aspect of life has opened the door to threats in cyberspace. Criminal elements inside and outside organizations gain access to information that can cause financial and reputational damage. Criminals also target individuals daily with personal devices like smartphones and home security systems who are often unaware of the dangers and the privacy threats around them. The Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution is a critical scholarly resource that creates awareness of the severity of cyber information threats on personal, business, governmental, and societal levels. The book explores topics such as social engineering in information security, threats to cloud computing, and cybersecurity resilience during the time of the Fourth Industrial Revolution. As a source that builds on available literature and expertise in the field of information technology and security, this publication proves useful for academicians, educationalists, policy makers, government officials, students, researchers, and business leaders and managers.

The Cloud! It sounds fluffy and soft. Amorphous, remote, floating above the world. Run it in the Cloud, we say. A modern metaphor, but we once had another name, a more descriptive name for using someone elseÕs computer. We called it timesharing. Today we mix the idea of using distant computers and the idea of communicating via a network and call the combination The Cloud, imagining we have invented something new. But it isnÕt so new after all. Beginning in the 1960s, a company created a successful business making remote computer services available inexpensively to anyone via a network built for that purpose. In doing so, they created the first cloud. Companies offered online resources from banking to research, email to instant messaging, and the ability to run applications on powerful, remote computers and access them from anywhere. They called it Tymnet, and the company was Tymshare.

Offers a critical look at the hyperbole surrounding the Internet and the future uses of computer networks, and discusses the false assumptions concerning the true benefits of computers

In this text the author looks at the battle between the computer underground and the security industry. He talks to people on both sides of the law about the practicalities, objectives and wider implications of what they do.

Violent Python shows you how to move from a theoretical understanding of offensive computing concepts to a practical implementation. Instead of relying on another attacker's tools, this book will teach you to forge your own weapons using the Python programming language. This book demonstrates how to write Python scripts to automate large-scale network attacks, extract metadata, and investigate forensic artifacts. It also shows how to write code to intercept and analyze network traffic using Python, craft and spoof wireless frames to attack wireless and Bluetooth devices, and how to data-mine popular social media websites and evade modern anti-virus. Demonstrates how to write Python scripts to automate large-scale

network attacks, extract metadata, and investigate forensic artifacts Write code to intercept and analyze network traffic using Python. Craft and spoof wireless frames to attack wireless and Bluetooth devices Data-mine popular social media websites and evade modern anti-virus
Research on cybercrime has been largely bifurcated, with social science and computer science researchers working with different research agendas. These fields have produced parallel scholarship to understand cybercrime offending and victimization, as well as techniques to harden systems from compromise and understand the tools used by cybercriminals. The literature developed from these two fields is diverse and informative, but until now there has been minimal interdisciplinary scholarship combining their insights in order to create a more informed and robust body of knowledge. This book offers an interdisciplinary approach to research on cybercrime and lays out frameworks for collaboration between the fields. Bringing together international experts, this book explores a range of issues from malicious software and hacking to victimization and fraud. This work also provides direction for policy changes to both cybersecurity and criminal justice practice based on the enhanced understanding of cybercrime that can be derived from integrated research from both the technical and social sciences. The authors demonstrate the breadth of contemporary scholarship as well as identifying key questions that could be addressed in the future or unique methods that could benefit the wider research community. This edited collection will be key reading for academics, researchers, and practitioners in both computer security and law enforcement. This book is also a comprehensive resource for postgraduate and advanced undergraduate students undertaking courses in social and technical studies.
The internet is established in most households worldwide and used for entertainment purposes, shopping, social networking, business activities, banking, telemedicine, and more. As more individuals and businesses use this essential tool to connect with each other and consumers, more private data is exposed to criminals ready to exploit it for their gain. Thus, it is essential to continue discussions involving policies that regulate and monitor these activities, and anticipate new laws that should be implemented in order to protect users. Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications examines current internet and data protection laws and their impact on user experience and cybercrime, and explores the need for further policies that protect user identities, data, and privacy. It also offers the latest methodologies and applications in the areas of digital security and threats. Highlighting a range of topics such as online privacy and security, hacking, and online threat protection, this multi-volume book is ideally designed for IT specialists, administrators, policymakers, researchers, academicians, and upper-level students.
A simultaneous Traditional Chinese translation of the much talked about book No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State by Glenn Greenwald. The book is the winner of the 2014 Pulitzer Prize for Public Service. In Traditional Chinese. Annotation copyright Tsai Fong Books, Inc. Distributed by Tsai Fong Books, Inc.