

BeagleBone provides a reader-friendly guide to the device, including a crash course in computer engineering. While following step by step, you can: Get up to speed on embedded Linux, electronics, and programming Master interfacing electronic circuits, buses and modules, with practical examples Explore the Internet-connected BeagleBone and the BeagleBone with a display Apply the BeagleBone to sensing applications, including video and sound Explore the BeagleBone's Programmable Real-Time Controllers Updated to cover the latest Beagle boards, Linux kernel versions, and Linux software releases. Includes new content on Linux kernel development, the Linux Remote Processor Framework, CAN bus, IoT frameworks, and much more! Hands-on learning helps ensure that your new skills stay with you, allowing you to design with electronics, modules, or peripherals even beyond the BeagleBone. Insightful guidance and online peer support help you transition from beginner to expert as you master the techniques presented in Exploring BeagleBone, the practical handbook for the popular computing platform.

Forensic Computing Anthony Sammes 2007-08-18 In the second edition of this very successful book, Tony Sammes and Brian Jenkinson show how the contents of computer systems can be recovered, even when hidden or subverted by criminals. Equally important, they demonstrate how to insure that computer evidence is admissible in court. Updated to meet ACPO 2003 guidelines, Forensic Computing: A Practitioner's Guide offers: methods for recovering evidence information from computer systems; principles of password protection and data encryption; evaluation procedures used in circumventing a system's internal security safeguards, and full search and seizure protocols for experts and police officers.

Network Programming with Perl Lincoln D. Stein 2001 A text focusing on the methods and alternatives for designed TCP/IP-based client/server systems and advanced techniques for specialized applications with Perl. A guide examining a collection of the best third party modules in the Comprehensive Perl Archive Network. Topics covered: Perl function libraries and techniques that allow programs to interact with resources over a network. IO: Socket library ; Net: FTP library -- Telnet library -- SMTP library ; Chat problems ; Internet Message Access Protocol (IMAP) issues ; Markup-language parsing ; Internet Protocol (IP) broadcasting and multicasting.

The Executive MBA in Information Security John J. Trinckes, Jr. 2011-06-03 According to the Brookings Institute, an organization's information and other intangible assets account for over 80 percent of its market value. As the primary sponsors and implementers of information security programs, it is essential for those in key leadership positions to possess a solid understanding of the constantly evolving fundamental concepts of information security management. Developing this knowledge and keeping it current however, requires the time and energy that busy executives like you simply don't have. Supplying a complete overview of key concepts, The Executive MBA in Information Security provides the tools needed to ensure your organization has an effective and up-to-date information security management program in place. This one-stop resource provides a ready-to use security framework you can use to develop workable programs and includes proven tips for avoiding common pitfalls—so you can get it right the first time. Allowing for quick and easy reference, this time-saving manual provides those in key leadership positions with a lucid understanding of: The difference between information security and IT security Corporate governance and how it relates to information security Steps and processes involved in hiring the right information security staff The different functional areas related to information security Roles and responsibilities of the chief information security officer (CISO) Presenting difficult concepts in a straightforward manner, this concise guide allows you to get up to speed, quickly and easily, on what it takes to develop a rock-solid information security management program that is as flexible as it is secure.

Apache HTTP Server 2.2 Official Documentation - Volume II. Security and Server Programs Apache Software Foundation 2010-04 The Apache HTTP Server 2.2 Official Documentation books covers all aspects of using and managing for the world's most popular web server. **Cyber Operations** Mike O'Leary 2019-03-01 Know how to set up, defend, and attack computer networks with this revised and expanded second edition. You will learn to configure your network from the ground up, beginning with developing your own private virtual test environment, then setting up your own DNS server and AD infrastructure. You will continue with more advanced network services, web servers, and database servers and you will end by building your own web applications servers, including WordPress and Joomla!. Systems from 2011 through 2017 are covered, including Windows 7, Windows 8, Windows 10, Windows Server 2012, and Windows Server 2016 as well as a range of Linux distributions, including Ubuntu, CentOS, Mint, and OpenSUSE. Key defensive techniques are integrated throughout and you will develop situational awareness of your network and build a complete defensive infrastructure, including log servers, network firewalls, web application firewalls, and intrusion detection systems. Of course, you cannot truly understand how to defend a network if you do not know how to attack it, so you will attack your test systems in a variety of ways. You will learn about Metasploit, browser attacks, privilege escalation, pass-the-hash attacks, malware, man-in-the-middle attacks, database attacks, and web application attacks. What You'll Learn Construct a testing laboratory to experiment with software and attack techniquesBuild realistic networks that include active directory, file servers, databases, web servers, and web applications such as WordPress and Joomla!Manage networks remotely with tools, including PowerShell,

WMI, and WinRMUse offensive tools such as Metasploit, Mimikatz, Veil, Burp Suite, and John the RipperExploit networks starting from malware and initial intrusion to privilege escalation through password cracking and persistence mechanismsDefend networks by developing operational awareness using auditd and Sysmon to analyze logs, and deploying defensive tools such as the Snort intrusion detection system, IPFire firewalls, and ModSecurity web application firewalls Who This Book Is For This study guide is intended for everyone involved in or interested in cybersecurity operations (e.g., cybersecurity professionals, IT professionals, business professionals, and students) **Principles of Information Security** Michael E. Whitman 2011-01-01 The fourth edition of Principles of Information Security explores the field of information security and assurance with updated content including new innovations in technology and methodologies. Students will revel in the comprehensive coverage that includes a historical overview of information security, discussions on risk management and security technology, current certification information, and more. The text builds on internationally-recognized standards and bodies of knowledge to provide the knowledge and skills students need for their future roles as business decision-makers. Information security in the modern organization is a management issue which technology alone cannot answer; it is a problem that has important economic consequences for which management will be held accountable. Students can feel confident that they are using a standards-based, content-driven resource to prepare for their work in the field. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Network Design Teresa C. Piliouras 2004-12-28 There are hundreds of technologies and protocols used in telecommunications. They run the full gamut from application level to physical level. It is overwhelming to try to keep track of them. Network Design, Second Edition: Management and Technical Perspectives is a broad survey of the major technologies and networking protocols and how they inter **The Food Chain** Barbara Krasner 2018-12-15 Globalization has impacted many aspects of life, and the food chain is no exception. Approximately one-quarter of America's food supply is imported, and while food production and manufacturing companies financially benefit from sourcing food from other countries, regulating these food sources becomes increasingly difficult. How does food regulation and inspection differ between countries? What can be done to ensure food imported from other countries is safe for consumption, and how can we make sure people involved in the food production process around the world are treated ethically? Readers will explore the many considerations affecting the global food chain.

The Internet Encyclopedia Hossein Bidgoli 2004 The Internet Encyclopedia in a 3-volume reference work on the internet as a business tool, IT platform, and communications and commerce medium.

AVIEN Malware Defense Guide for the Enterprise David Harley 2011-04-18 Members of AVIEN (the Anti-Virus Information Exchange Network) have been setting agendas in malware management for several years: they led the way on generic filtering at the gateway, and in the sharing of information about new threats at a speed that even anti-virus companies were hard-pressed to match. AVIEN members represent the best-protected large organizations in the world, and millions of users. When they talk, security vendors listen: so should you. AVIEN's sister organization AVIEWS is an invaluable meeting ground between the security vendors and researchers who know most about malicious code and anti-malware technology, and the top security administrators of AVIEN who use those technologies in real life. This new book uniquely combines the knowledge of these two groups of experts. Anyone who is responsible for the security of business information systems should be aware of this major addition to security literature. * "Customer Power" takes up the theme of the sometimes stormy relationship between the antivirus industry and its customers, and tries to dispel some common myths. It then considers the roles of the independent researcher, the vendor-employed specialist, and the corporate security specialist. * "Stalkers on Your Desktop" considers the thorny issue of malware nomenclature and then takes a brief historical look at how we got here, before expanding on some of the malware-related problems we face today. * "A Tangled Web" discusses threats and countermeasures in the context of the World Wide Web. * "Big Bad Bots" tackles bots and botnets, arguably Public Cyber-Enemy Number One. * "Crème de la CyberCrime" takes readers into the underworld of old-school virus writing, criminal business models, and predicting future malware hotspots. * "Defense in Depth" takes a broad look at DiD in the enterprise, and looks at some specific tools and technologies. * "Perilous Outsorcery" offers sound advice on how to avoid the perils and pitfalls of outsourcing, incorporating a few horrible examples of how not to do it. * "Education in Education" offers some insights into user education from an educationalist's perspective, and looks at various aspects of security in schools and other educational establishments. * "DIY Malware Analysis" is a hands-on, hands-dirty approach to security management, considering malware analysis and forensics techniques and tools. * "Antivirus Evaluation & Testing" continues the D-I-Y theme, discussing at length some of the thorny issues around the evaluation and testing of antimlware software. * "AVIEN & AVIEWS: the Future" looks at future developments in AVIEN and AVIEWS. * Unique, knowledgeable, unbiased and hype-free commentary. * Written by members of the anti-malware community; most malware books are written by outsiders. * Combines the expertise of truly knowledgeable systems administrators and managers, with that of the researchers who are most experienced in the analysis of malicious code, and the development and maintenance of defensive programs.