Since the first edition of this classic reference was published, World Wide Web use has exploded and e-commerce has become a daily part of business and personal life. As Web use has grown, so have the threats to our security and privacy--from credit card fraud to routine invasions of privacy by marketers to web site defacements to attacks that shut down popular web sites. Web Security, Privacy & Commerce goes behind the headlines, examines the major security risks facing us today, and explains how we can minimize them. It describes risks for Windows and Unix, Microsoft Internet Explorer and Netscape Navigator, and a wide range of current programs and products. In vast detail, the book covers:

Web technology--The technological underpinnings of the modern Internet and the cryptographic foundations of e-commerce are discussed, along with SSL (the Secure Sockets Layer), the significance of the PKI (Public Key Infrastructure), and digital identification, including passwords, digital signatures, and biometrics.

Web privacy and security for users--Learn the real risks to user privacy, including cookies, log files, identity theft, spam, web logs, and web bugs, and the most common risk, users' own willingness to provide e-commerce sites with personal information. Hostile mobile code in plug-ins, ActiveX controls, Java applets, and JavaScript, Flash, and Shockwave programs are also covered.

Web server security--Administrators and service providers discover how to secure their systems and web services. Topics include CGI, PHP, SSL certificates, law enforcement issues, and more.

Web content security--Zero in on web publishing issues for content providers, including intellectual property, copyright and trademark issues, P3P and privacy policies, digital payments, client-side digital signatures, code signing, pornography filtering and PICS, and other controls on web content.

Nearly double the size of the first edition, this completely updated volume is destined to be the definitive reference on Web security risks and the techniques and technologies you can use to protect your privacy, your organization, your system, and your network.

Most Helpful Customer Reviews


There are two basic reasons why a book comes out in a second edition: either the author needs the cash or the book needs to be updated. When the first edition of Web Security, Privacy & Commerce came out in 1997, it was titled Web Security & Commerce. Not only has the title changed, but Web security, privacy, and commerce have changed radically in the last five years.

The nature of the change and the pace at which it occurs is a large part of the difficulty within information security. Imagine a heart surgeon going on an extended vacation in 1997 and coming back in 2002. Although his surgical technique may be a bit rusty, there is no reason to think that he could not start practicing medicine again right away. However, if you were to take a contemporary information security professional from 1997 and place him in the 2002 workplace, he would be horribly outdated. Technologies that did not exist in 1997, or even 2000, are now ubiquitous, and technologies that were considered cutting edge only a few years ago are now archaic.

With that, the update to Web Security, Privacy & Commerce is indeed warranted and welcomed. A glance at the table of contents reveals coverage of nearly every core aspect within Web security. The book provides a comprehensive and impartial look at the technologies and approaches that both management and systems administrators can employ to ensure the security of their networks and systems. The author's impartiality is revealed in chapter 15, which describes several telephone scanner utilities; Garfinkel is the creator of one of the utilities, but makes sure to list the competition (and even has nice things to say about them).

Simson Garfinkel and Gene Spafford are veterans in the computer security world. Garfinkel is the author of several highly acclaimed books, and Spafford is a professor of computer science at Purdue University. Their succinct writing style allows them to cover a huge amount of information in a little over 700 pages.

The book is divided into four sections: Web technology, privacy and security for users, Web server security, and security for content providers. Part one goes into details about the security foundations of the networks and the Internet. Topics include SSL/TLS, PKI, digital signatures, and biometrics. These seven chapters give the reader a good overview of the essence of information security.

Part 2, "Privacy and Security for Users," is quite different from other security books. Whereas other books detail the problems with privacy on the Internet, this book does a good job of showing users various strategies for keeping their personal information private. Garfinkel shows how the real threats to personal
privacy are not so much cookies and log files; rather the end-users very own readiness to provide Web and e-commerce sites with their personal information. Part 3, “Web Server Security,” details how service providers and systems administrators can lock down and secure their systems. The authors provide details on topics such as host security, server access methods, and secure CGI/API programming. Part 4, “Security for Content Providers,” is quite interesting, as many content providers and ISPs forget that the onus of security and privacy to a large degree falls on them. This section includes details on how these providers can use various techniques, from filters to PICS and more, to ensure their users’ privacy. The fact that Web Security, Privacy & Commerce, 2nd Edition, is nearly twice the size of the first edition is indicative of the fact that security has changed radically since 1997. Whether you run a Web site or are concerned about security for your PC at home, Web Security, Privacy & Commerce is a must read.

I work as a computer security analyst for a major consulting firm. Garfinkel’s book is head and shoulders above anything else out there. In particular, his handling of the tension between security policy and privacy policy is particularly well written. I highly recommend this book to anyone that wants to develop a detailed understanding of the significant issues that affect doing business on the web.

Apart from paid reviewers I can’t see anyone with any actual knowledge of security rating this book 5 stars. It is not as clear and concise as it should be, and the technical knowledge is freely available at securityfocus.com and other sites. A better job could have been done with security and privacy policies. More effort should have been put forth in providing common sense (implementable) solutions or best practices instead of re-hashing material that other books have already done a better job presenting. I normally enjoy O’reilly books but like the first edition, this book is a disappointment.

Good read, but primarily as an introductory primer. General info and comprehensive, with good discussion and resources. But to really get into the nuts and bolts of this subject, you will need to find other books. Somewhat esoteric at times and frustrating.

Ever since the birth of the World Wide Web, we have been inundated with books purporting to have all things “Internet”, buying into the hype surrounding the explosion of the web. What these books failed to do was educate people about the lack security and privacy inherent on the Internet, That is why I was wanted to read “Web Security, Privacy and Commerce: 2nd Edition” (734 pages (I do not count an index in the page count), O’Reilly Media, 2002, ISBN 0-596-00045-6). Written by Simon Garfinkel, with Gene Spafford, I read more and more with pleasure and anticipation. This was confirmed with a simple line that has often been lost on the masses: the Internet was built for communication and sharing, not for business and the protection of data at each end of the connection. Unfortunately, the explosive growth of the Web did not allow for this issue to be fully addressed or for reliable tools to be built quickly enough. Now other reviews I have read on here blast the book for being too generic and not what they expected from O’Reilly. But that is what I find to be a breath of fresh air: a wide-ranging important topic that does not get bogged-down in techno-speak, something which might normally turn readers away from technical books. From the outset, Garfinkel and Spafford tell you that their goal is to cover the fundamentals of web security and not to be a primer for “computer security, operating systems, or the World Wide Web”. Do they succeed in their goal? Absolutely! Starting with web technology, they address security, web architecture, cryptography (what it is and what it isn’t), SSL and digital identification. They then move onto privacy and security for users in very simple, direct, tell it like it is style. How many people know what “Joes” are and the fact that anyone could look at their users and find at least one? How often have you read that using a 16 character password is counterproductive and that if chosen correctly, an 8 character password should be more than adequate? When is the last time you had an author break down cookies line by line for you to truly understand them? Have you ever tried to find out what the code inside a worm is and does? As they weave their story, they then cover Web Server Security and offer a very compelling argument for using a Mac with OS 7, 8 or 9 for a server (I won’t give away the reason why here or tell you that Rosebud is a sled). For the programmer, this section offers a street-smart view of coding vulnerabilities and ways to minimize them. In addition, they cover physical security, as well as host security, for servers. Want to really understand SSL and certificates and want to know why Netscape 4 was a bad example of certificate planning? I had never thought about it until reading their discussion of the topic. They finish up with coverage of security for content providers. What is very, very good here is that they cover privacy policies, filtering, censorship.
and intellectual property. They help you truly understand what fair use is and what it really means. The only negative I had was too short a discussion on Social Engineering. However, given the fact that this was published in 2002 and phishing scams had not really taken off raising awareness of the issue, I am giving them a mulligan for this. The ideal audience for this book is people who need to have a broad understanding without nitty-gritty detail that they will get lost in. How good a reference do I find this book to be? Well for starters, I wished I had it at my side when preparing for the Certified Information Systems Auditor (CISA) Exam offered by the Information Systems Audit and Control Association (ISACA). It puts their review materials to shame (have to be honest about that). This book will be part of my permanent library and will be required reading for any information systems auditors doing work for my company. I will also be using this book as a source text for training provided to companies, developers, and administrators.

The Business Control Caddy Scorecard: Double-Eagle on a Par 5.

Christopher Byrne, IBM CAAD/CASA

The Business Controls Caddy (tm)...

Read more ›

except for the underlying theory about cryptography that is actually not the target content for the reader of this book, all the contents are out-dated severely in a word. The author should rewrite the significant part of this book for readers. Great book! It provided me with the information that I was looking for and is an easy read. Not every book has all of the information that you may need, but it is definitely a good...

Read more

This book is easy to read and describes basic security principles and technologies in an understandable manner. If you're looking for an intro to security book, this is a good one.

I think this is another one of those big books that tries to cover too many topics. It's really just a general discussion about web security, rather than a handbook of any kind. This edition is from 2002...10 years old on a topic evolving every week. Read more

Web Security, Privacy and Commerce by Simson Garfinkel, Gene Spafford was a gift to me for my birthday when getting ready to pass my “Master Site Designer,” test it... Read more