Open Systems and Standards for Software Product Development

P.A. Dargan, Artech House, 2005, \$89.00, ISBN: 1580537499

Open Systems and Standards for Software Product Development aims to provide software project managers, enterprise managers, systems and communications engineers, and product vendors with relevant information on open systems and standards. It describes a framework for understanding the state of the art of stan-

dards. In that process, author P. A. Dargan has produced a compendium of standards for open systems. The term *open systems* refers to systems built using commercial off-the-shelf products. Open systems should be based on standards that specify the basic modules in terms of their reusability, interconnectivity, interoperability, and easy upgradeability.

The first two chapters elaborate on the concepts of open systems and standards and their relevance to software developers. Chapters 3 through 14 cover 12 areas of technology where standards compliance is critical. The author discusses major standards in each area using a template that consists of: the name of the standard, its intended function, its history, the organization responsible for the standard, current status, source for obtaining the specifications, Web site for the standard, list of vendors and products, and other sources of information.

The chapter on applications discusses six standards related to electronic business, including business process execution language for Web services (specifies business-process models, interaction, and protocols); business process modeling, notation, and language (defines standards based on XML to provide a common notation and language for modeling business process); and RosettaNet (defines a suite of standards to support e-business exchanges). The chapter on communications discusses standards for asynchronous transfer, Ethernet, Internet, VoIP, Bluetooth, and Wi-Fi, among others.

In the concluding chapter, the author identifies five key trends that highlight Internet and Web-based standards that are expected to accomplish the open systems vision: high-speed, ubiquitous communications; better security mechanisms; intelligent push/pull from data stores with capacities of petabytes; worldwide electronic

collaboration; and seamless interfaces to networked applications, data, and computers.

References are supplied at the end of each chapter, and for every standard discussed, an extensive list of Web sites is provided. *Open Systems and Standards for Software Product Development* is bound to become indispensable to project managers, systems and communications engineers, and chief information officers.—A. K. Menon

Intrusion Prevention and Active Response: Deploying Network and Host IPS

Michael Rash, Angela D. Orebaugh, Graham Clark, Becky Pinkard, Jake Babbitt, Syngress Publishing, 2005, \$49.99, ISBN: 193226647X

Intrusion prevention is one of the most popular security buzz phrases of the last few years. There has been a limited amount of literature discussing the prevention side of intrusion detection, but this book makes a great contribution to understanding the underlying concepts and possibilities, as well as

the limitations of IPS (intrusion prevention system).

Though this book is excellent, it does have two limitations. First, it starts on a technical level that is inaccessible to everyone but security professionals. For all newcomers to the security field, I recommend starting with a different book. The book's second limitation is its focus on open source products and implementations. It contains some material about Internet Information Services and other Windows-related topics, but if you want to know how to protect your Windows machines on an operating system level, this is the wrong book.

The book has a really nice hands-on approach, and the theoretical explanations are well done. The authors show the basics of intrusion detection, the evolution to intrusion prevention, and how this technique can be dangerous regarding false positives and active response. The authors provide nice explanations of host protection through the operating system, how to use IPS on the application layer, and how to deploy various open source solutions. I recommend this book to all technical security professionals who are interested in a competent explanation of today's open source IPS solutions and concepts, and who value a pragmatic approach.—Andreas Tomek

Reprinted from *Computing Reviews*, © 2005 ACM, <http://www.reviews.com>