Extrusion Detection: Security Monitoring for Internal Intrusions

Richard Bejtlich, Addison-Wesley Professional, 2005,
\$49.99, ISBN: 0321349962

Although most readers are probably familiar with the term *intrusion detection* and its general underlying function, they are probably not familiar with *extrusion detection*, a new concept that may become an emerging key technology in network security. Behind this concept is a series

of techniques and approaches for monitoring outbound connections in order to detect a potential intruder or a violation of in-place security policies. Outbound connections are initiated from your network toward the outside, and, at first glance, monitoring them seems to be just a simple and straightforward extension of general network monitoring.

Try to imagine, however, what would happen if you had to deploy an outbound monitoring architecture on a high-speed network. What hardware should you use? A simple FreeBSD box with some monitoring software might work well for a small enterprise, but will it work for a large campus network with high-speed connections in the gigabit range? Beyond having the right hardware, where would you install it? Should it be in the demilitarized zone, within the internal network, or in both?

Richard Bejtlich does a superb job addressing these questions and provides directly applicable solutions and precise technical answers. He starts by defining the scope and challenges of extrusion detection and then goes into all the required details and technical issues associated with it. The book covers the essentials, providing information on how to get the right hardware, how to install a multiport tap (including graphic illustrations), and how to deploy it correctly so that both the internal and the demilitarized networks are monitored. He also describes some traffic-specific analysis using open source tools (sguil, snort, argus, and sancp are the most important). An important part of the book is dedicated to describing defensible networks and implementing access control mechanisms.

I strongly recommend this book to any reader interested in intrusion detection, general network security, and network security monitoring. Difficult concepts

and technologies are clearly explained and abundantly illustrated with figures and do-it-yourself instructions. A reader with average skills can easily follow both the theoretical contents and the practical details.—*Radu State*

Grid Database Design

April Wells, Auerbach Publications, 2005, \$79.95,
ISBN: 0849328004

Grid computing will transform the way we use computers, says author April Wells in *Grid Database Design*. Today the Internet lets computers exchange information among themselves; tomorrow the grid will let them pool their computational power to solve problems together—problems too complex for any one computer to solve alone. All of the usual computer science concepts take on a new meaning in grid computing, and this book describes them all.

The book is divided into three parts. The first part is historical. It frames the emergence of grid computing as a somewhat natural evolution, from the first mainframes and the rise of PCs to the birth of the Internet and the first peer-to-peer applications (Napster and Gnutella), which are early examples of grid computing. It also describes the different kinds of grids that can be built (computational, data, and collaboration), and the environments where grids are already in use, including corporations, research institutions, and government.

The second part describes the components of a grid. If almost every piece of hardware can be part of a grid, there must also be some specialized software to let this hardware work together. Above all, there must be metadata, which is the glue that lets data created in heterogeneous environments share a common meaning within the grid.

The last part discusses database technology, starting with familiar database concepts, such as the relational and object database models, and moving on to parallel and distributed databases and data synchronization.

This book is an excellent introduction to grid computing for people who may have heard about it and want to understand it. The coverage, though not in depth, is broad and presents all relevant aspects of the technology. Familiarity with some database and general IT concepts is recommended.—*Andrea Paramithiotti*

Reprinted from *Computing Reviews*, © 2006 ACM, <http://www.reviews.com>