In the last few years, the term intrusion prevention system has proliferated both in academia and commercially. This has introduced in the security market some expectations—and also some confusion—regarding these devices’ potential and the risks an organization can incur by not having one installed. Despite the hype that often comes up around a new name, IPS refers not to a novel and revolutionary technology but merely to the integration of numerous existing security functionalities into a single platform. To some extent, dressing an existing product in new clothes is often a marketing maneuver aimed at overcoming criticisms of related technologies whose performance is far from what commercial advertisements promise (as with intrusion detection systems, or IDS).

As a security paradigm, intrusion prevention simply aims to detect and stop attacks. In practice, most IPS products strongly resemble firewalls. However, they usually include algorithms to perform more sophisticated traffic inspection and to operate at the application layer in addition to performing classic network and transport processing. To achieve this, developers have progressively incorporated scanning and checking functionalities—typical of devices such as IDS and antivirus—into firewalls. In other cases, a combination of these detection-and-response mechanisms is integrated into a single platform.

So, what exactly is an IPS? How does it differ from technologies such as IDS and application-layer firewalls? Intrusion Prevention and Active Response: Deploying Network and Host IPS, by Michael Rash, Angela Orebaugh, Graham Clark, Becky Pinkard, and Jake Babbin, is one of the first books to try to offer a comprehensive view of intrusion prevention technology.

**Audience and scope**

Intrusion Prevention and Active Response: Deploying Network and Host IPS isn’t an academic
book. If you’re looking for a theoretical engineering background on problems related to intrusion prevention (such as which features must be analyzed to detect an ongoing intrusion or how to respond automatically to an incident), this isn’t the text to seek out. Rash and his coauthors mostly concentrate on available tools and real-world techniques to detect and respond to intrusions, ranging from packet inspection and inline data modification to buffer overflow protection. As a result, much of the content will be familiar to those with network and systems security backgrounds, especially in IDS and firewalls.

The book requires some technical background in distributed systems and, particularly, in network protocols and applications. The authors provide numerous examples of explicit packet captures and traces, which greatly clarify some concepts. In addition to network intrusion prevention, the book devotes an entire section to host-oriented protection measures.

A flawed but practical approach
I found the book somewhat unfocused and unstructured, probably because intrusion prevention itself is still a disordered amalgam of techniques and technologies linked together solely to avoid intrusions. This doesn’t justify, however, the number of pages devoted to tangential matters, such as discussing nmap options. Moreover, it completely lacks references. The pointers to related sites and free tools are useful, but every decent book should offer a list of additional readings for those who want to deal with specific matters in depth.

However, the book provides nice, practical coverage of packet inspection techniques for intrusion analysis and network inline data modification. I especially enjoyed chapter 8, “Deploying Open Source IPS Solutions,” which applies many of the book’s concepts to a real scenario. This material is useful in clarifying IPS technology’s capabilities.

To date, hardly a handful of books are devoted exclusively to IPS technology. Rash and his coauthors have performed a remarkable effort in putting together the most relevant techniques and tools, resulting in a good starting point for those wanting to learn how this technology works.

*Intrusion Prevention and Active Response: Deploying Network and Host IPS* provides a practical overview of the main principles and tools available in this discipline. Despite the cons I discussed earlier, the material would be valuable for network architects and security administrators who might have to consider whether to deploy an IPS in their organization and how to deal with its practical implications.

**Juan M. Estevez-Tapiador** is an associate professor in Carlos III University of Madrid’s Computer Science Department. Contact him at tapiador@ieee.org.
Related Links

- "Building Dependable Intrusion Prevention Systems," Int'l Conf. Dependability of Computer Systems
- "Building Intrusion-Tolerant Secure Software," Int'l Symp. Code Generation and Optimization

Cite this article: